UNIVERSITY OF PLYMOUTH

Authentication Technologies

Dr Hai-Van Dang

Centre for Security, Communications and Network Research

Learning outcome checklist

1. Recognize the approach of an authentication protocol [1]
2. Create a strong password, keep and use it safely [2]
3. Consider to improve an authentication system security [4]
4. Analyze password-based authentication: pros, cons, attack vectors, counter measures [1]
5. Analyze the use of a token-based authentication: pros, cons, attack vectors, counter measures [1]
6. Analyze the use of biometrics-based authentication: pros, cons, attack vectors, counter measures [1,3]
7. Compare the security and usability of biometric-based authentication systems based on FAR and FRR [1]
8. Understand how Single Sign On works [5,6]
9. Tell the difference between cookie-based authentication and SSO [7]

Further reading

1. Transparent User Authentication: Biometrics, RFID and Behavioural Profiling (online version in Primo, accessible from DLE): read section 1.3, 4.2, 4.3, 4.4
2. https://www.ncsc.gov.uk/cyberaware/home
3. https://www.ncsc.gov.uk/collection/biometrics
4. https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach
5. https://auth0.com/blog/what-is-and-how-does-single-sign-on-work/
6. https://www.youtube.com/watch?v=51B-jSOBF8U
7. https://www.youtube.com/watch?v=GhrvZ5nUWNg
8. BBC iplayer, The Secret Genius of Modern Life, series 1:1 Bank card

Session Content

Overview

Secret-based approaches

Token-based approaches

Biometrics

Future Authentication

Conclusions

CIA AAA…?

- Confidentiality
- Integrity
- Availability

- **Authentication**
- Authorisation
- Accountability

User Identification and Authentication

Menti.com

1. What is identification and why systems need it?
2. What is authentication and why systems need it?
3. How many online accounts do you have?
4. How are you authenticated to your online accounts?

User Identification and Authentication

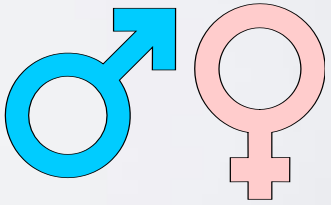
- Users must be identified to enable :
  - user-specific access controls
  - individual accountability for activities
- *Claimed* identities must be *authenticated* :
  - first line of system protection
  - safeguards against abuse by external parties or unauthorised insiders

A multitude of identities

- Plethora of accounts requiring authentication
  - regular use of 20+ online services requiring authentication is not unusual
  - this number could easily double with sites that are used occasionally
- Often not authenticating for a true security purpose
  - login enables the *provider* to track usage rather than helping the user to protect an asset
  - Users end up with more accounts to manage without a real personal benefit

Authentication factors (Authentication methods)

- Three main approaches:
  - Something the user *knows* (e.g. passwords and PINs)
  - Something the user *has* (e.g. a card or token)
  - Something the user *is* (i.e. a biometric)



Authentication approach – Example 1

- Menti
- Recognize the authentication factors in the following scenario:

A 10-person consulting firm sent a small team to South America to complete a client project. During their stay, an employee used a business debit card at a local ATM.

Authentication approach – Example 2

- Menti
- Recognize the authentication factors in the following scenario:

A small family-owned construction company made extensive use of online banking and automated clearing house (ACH) transfers. Employees logged in with both a company and user-specific ID and password. Two challenge questions had to be answered for transactions over $1,000.

Authentication approach – Example 3

- Menti
- Recognize the authentication factors in the following scenario:

Iphone can be opened with FaceID

Ability to support alternatives

- Passwords and PINs are the baseline methods
  - recognised weaknesses and constraints, but it is hard to go beyond them
- Stronger approaches typically require additional technologies
  - biometrics (e.g. fingerprint, face, voice, iris)
  - tokens (e.g smart cards, RSA SecurID)
- Cannot rely upon users having them unless the service provider supplies them
  - even then some technologies will not work on all devices
- Upshot is that we generally end up relying upon methods that only depend upon a keyboard

Passwords

Passwords . . . are DEAD!

Activity

Menti

1. How many passwords do you have?
2. How do you manage your passwords?

Analyze password-based authentication

- Group work, 3-4 students per group (7 mins)

1. What are cons of passwords?
2. What are pros of passwords?
3. What can be attacks (at least 2) against password?
4. What are your suggestions to mitigate some of the mentioned attacks (at least 2)?

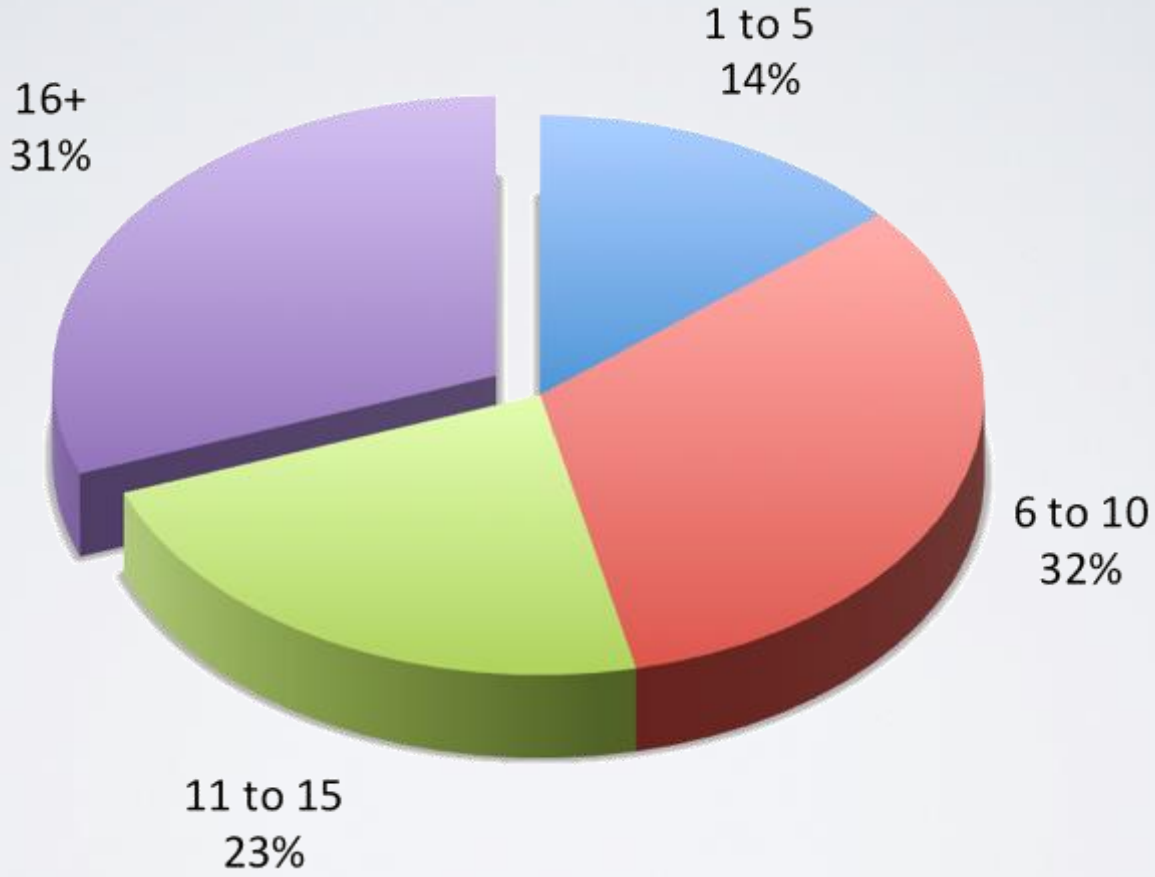
Traditional Passwords / PINs

- Pros
  - Easy to get the idea
  - Familiar from other systems
  - Can be made to work in most contexts (devices/systems/sites)

- Cons
  - Hard to use and manage properly (incl. memorability)
  - Inconvenient and time-consuming to enter (esp. for ‘strong’ passwords)

Lots to remember?

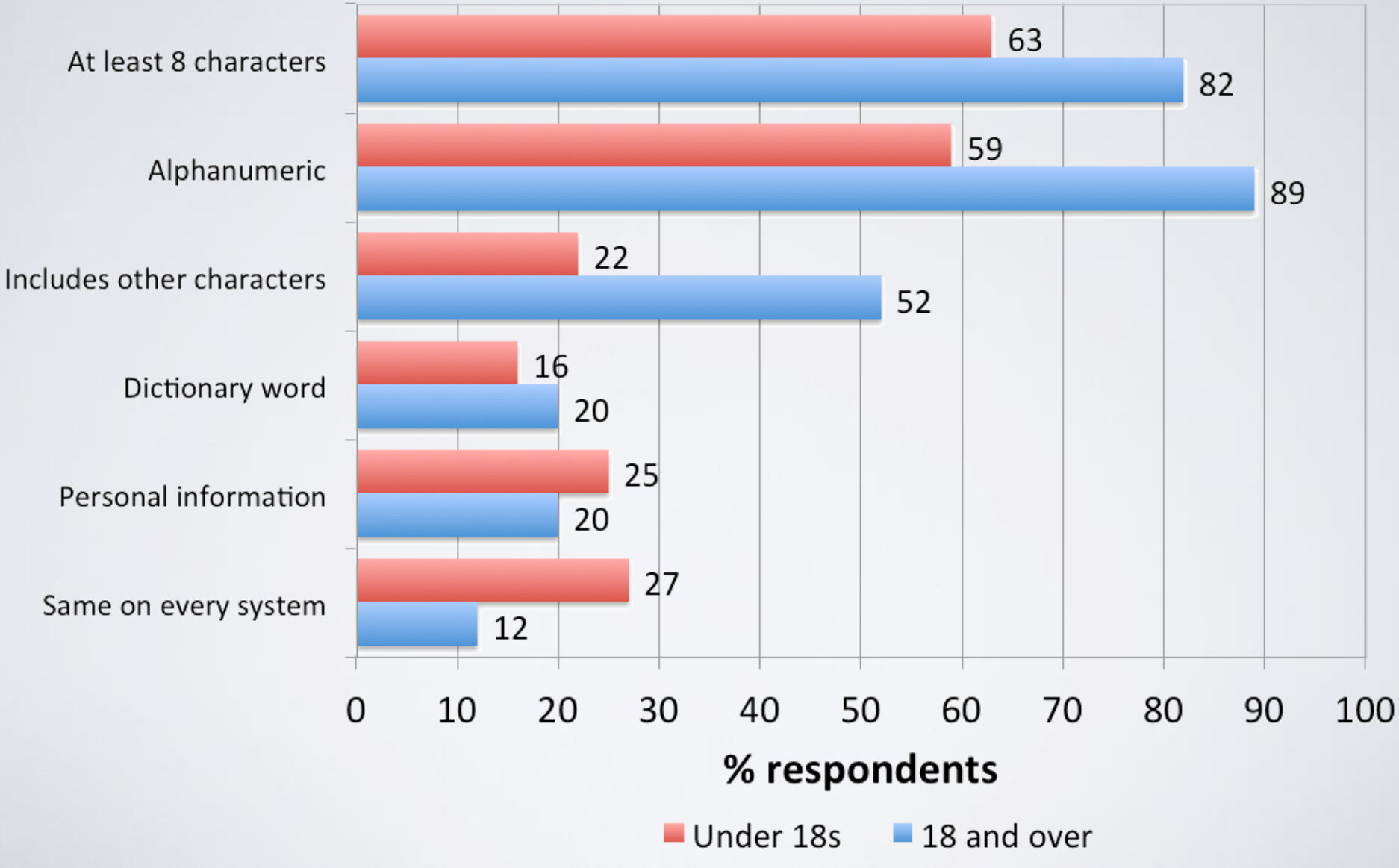
How many passwords?



(Furnell and Bär, 2012)

Based on 246 respondents

Password Practices



Reflection

1. How you create passwords – Password strength
2. How you manages passwords – Memory, notebook, password manager
3. How you use passwords – how often you change passwords, use similar or different passwords across the systems, share passwords with friends/ family or not,…

Predictably Popular

	2014	2015	2016	2017
1	123456	123456	123456	123456
2	password	password	password	password
3	12345	12345678	12345	12345678
4	12345678	qwerty	12345678	qwerty
5	qwerty	12345	football	12345
6	123456789	123456789	qwerty	123456789
7	1234	football	1234567890	letmein
8	baseball	1234	1234567	1234567
9	dragon	1234567	princess	football
10	football	baseball	1234	iloveyou

Source: SplashData

(see www.teamsid.com/worst-passwords-2017-full-list)

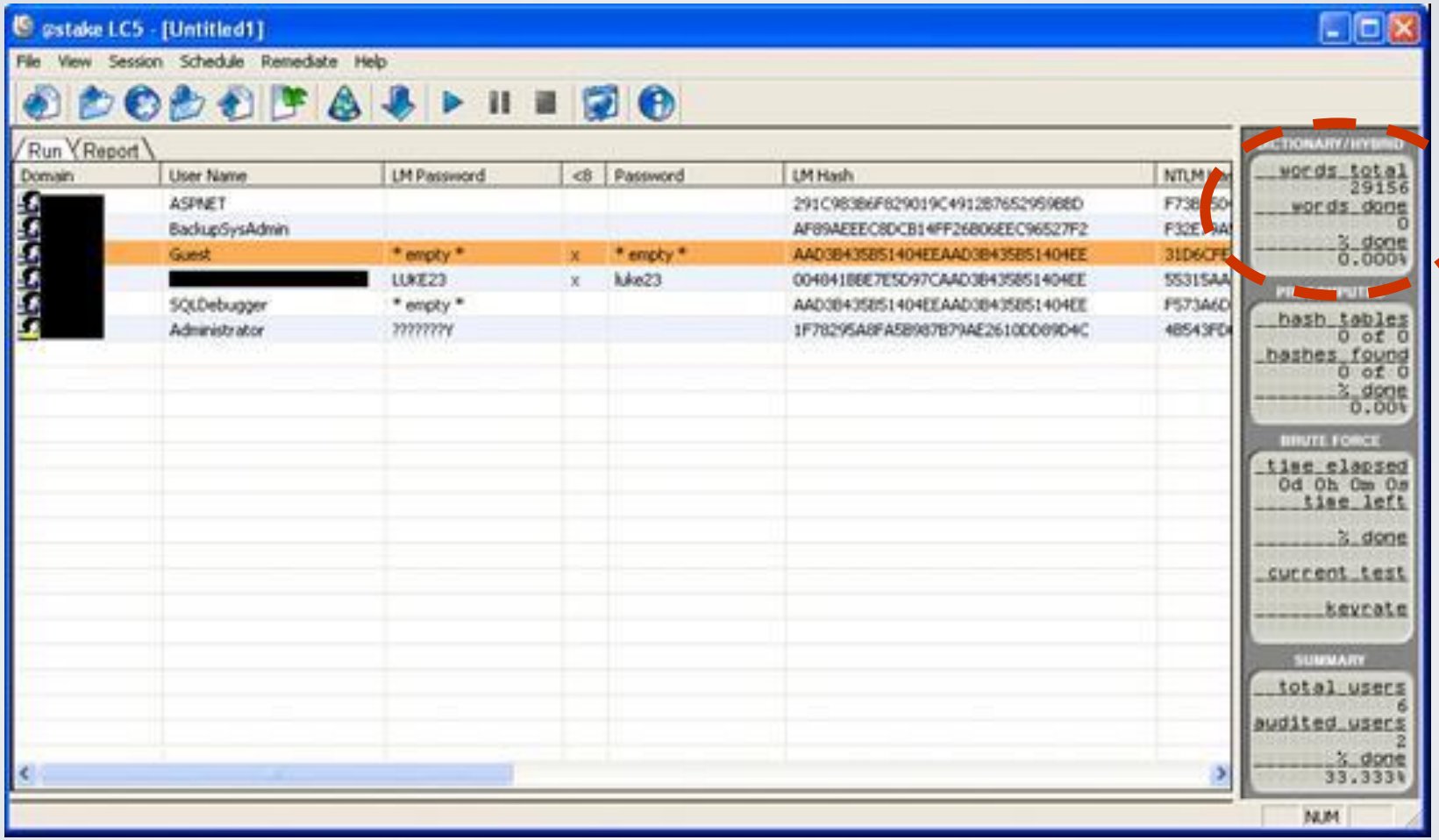
Table 1.4 Top 20 most common passwords

Analysis of 34,000 passwords (Schneier 2006)		Analysis of 32 million passwords (Imperva 2010)		
Rank	Password	Rank	Password	Number of users
1	password1	1	123456	290731
2	abc123	2	12345	79078
3	myspace1	3	123456789	76790
4	password	4	Password	61958
5	blink182	5	iloveyou	51622
6	qwerty1	6	princess	35231
7	fuckyou	7	rockyou	22588
8	123abc	8	1234567	21726
9	baseball1	9	12345678	20553
10	football1	10	abc123	17542
11	123456	11	Nicole	17168
12	soccer	12	Daniel	16409
13	monkey1	13	babygirl	16094
14	liverpool1	14	monkey	15294
15	princess1	15	Jessica	15162
16	jordan23	16	Lovely	14950
17	slipknot1	17	michael	14898
18	superman1	18	Ashley	14329
19	iloveyou1	19	654321	13984
20	monkey	20	Qwerty	13856

Password Weaknesses

- Passwords are often :
  - badly selected (and easily guessed):
    - too short
    - dictionary words
    - personal data (names, car registration etc.)
    - ➢ makes them vulnerable to password cracking tools and social engineering

Password cracking



Password Weaknesses

- More problems:
  - written down
  - infrequently (or never) changed
  - the same on multiple systems
  - only required at the start of a session (i.e. Point-of-entry authentication)
- And may also …
  - share them
  - forget them

Improving Password Systems

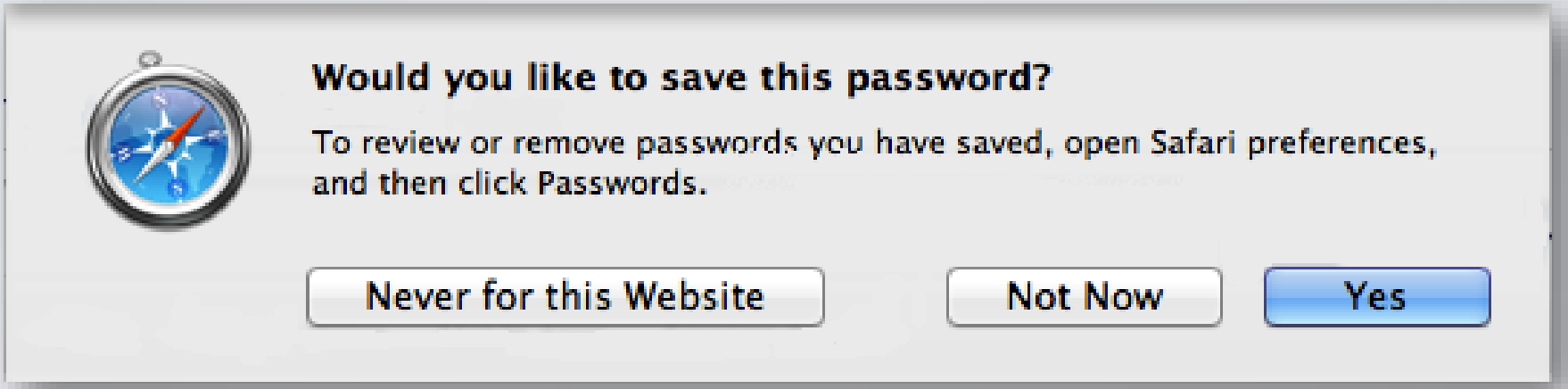
"Use them like a toothbrush.

Change them often and don't share them with friends"

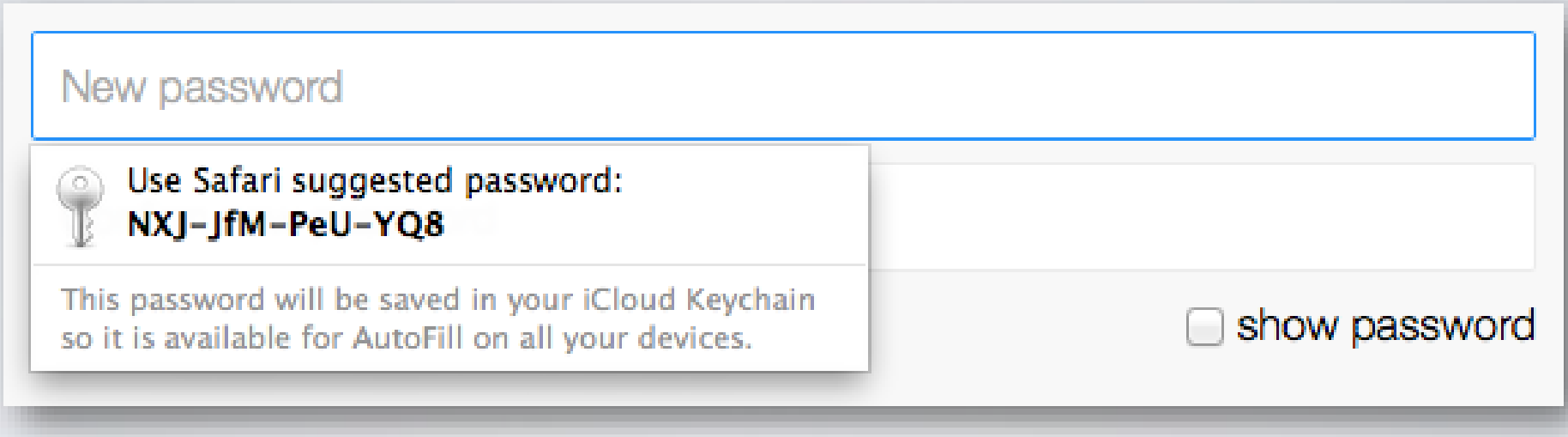
Cliff Stoll

IT security expert and author of "The Cuckoo's Egg"

What's the problem?

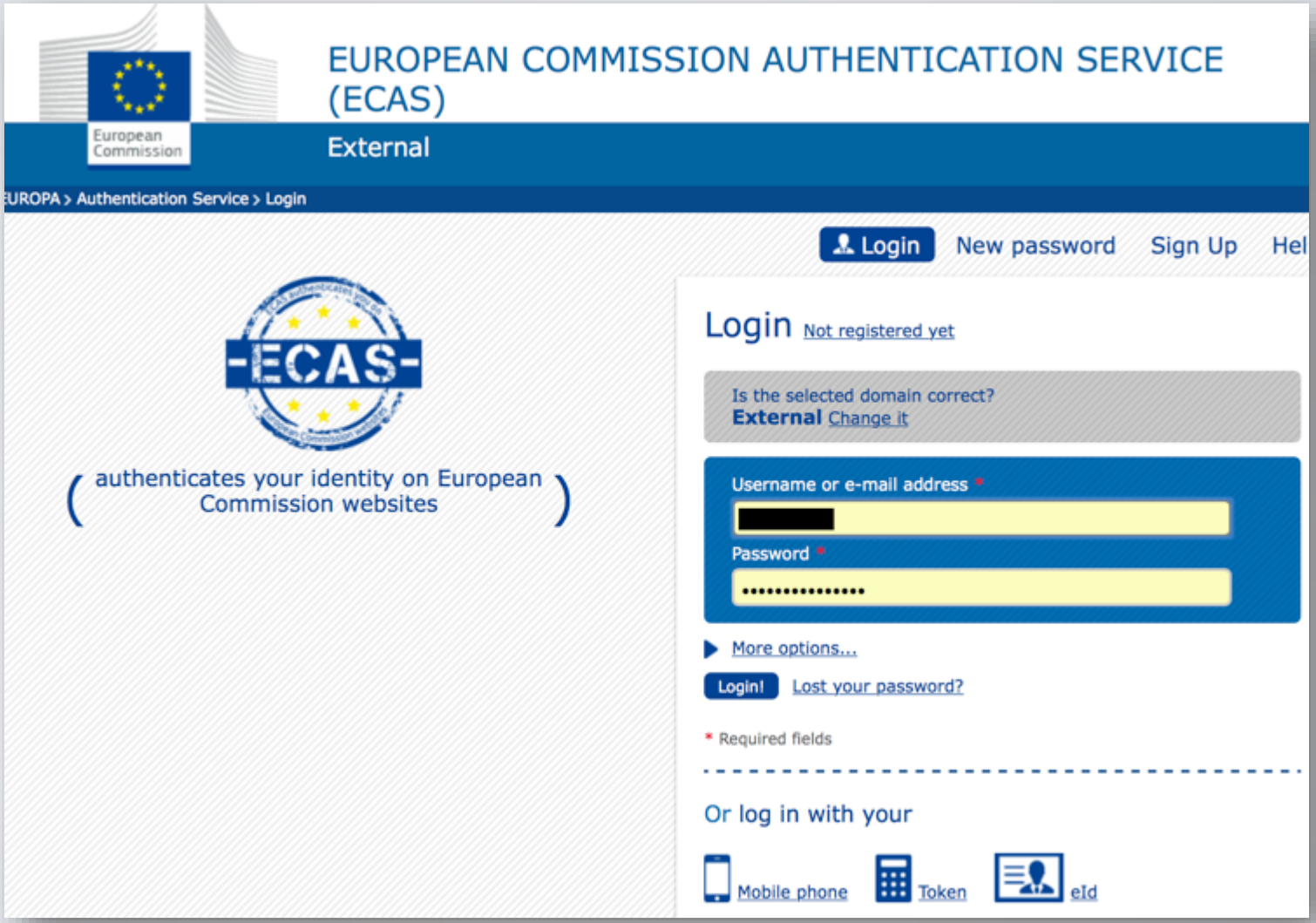


And what about here?



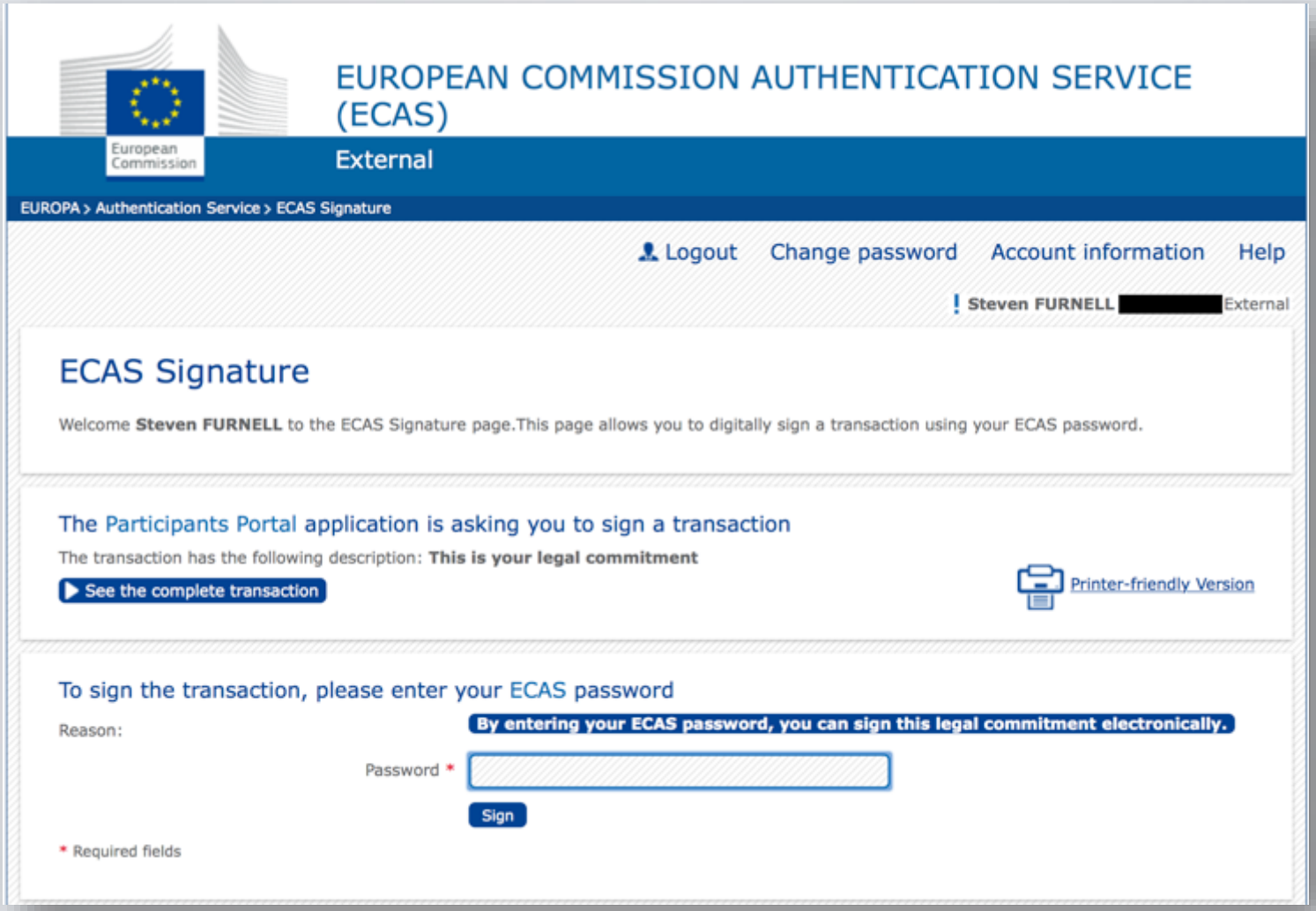
AutoFill in action

Provides it for me at Login …



AutoFill in action

… but *now* I need to remember the thing!



Which password is strong?

- Menti
- Which one of these passwords does not appear in the top 100,000 most compromised passwords?

a. arsenal22
b. p@55w0rd
c. victoria!
d. 1v7Upjw3nt
e. RedPantsTree
f. 20111977

Password selection guidelines by NCSC

- A good way to create strong, memorable passwords is by using 3 random words.
- Do not use words that can be guessed (like your pet’s name). You can include numbers and symbols if you need to.

https://www.ncsc.gov.uk/cyberaware/home

NCSC Password Tips

National Cyber Security Centre

Using passwords

To protect your devices & data

Passwords are an effective way to control access to your data, the devices you store it on, and the online services you use.This page contains tips about how to create strong passwords, how to look after them, and what to do if you think they've been stolen. For more information, please refer to www.cyberaware.gov.uk .

Criminals will use the most common passwords to try and access your accounts, or use information from your social media profiles to guess them. If successful, they will use this **same password** to try and access your **other accounts**.

Criminals also try and trick people into revealing their passwords by creating fake 'phishing' emails that link to **dodgy websites**, or by using **persuasive techniques** through social media.

Even if you create strong passwords (and look after them), they can still be **stolen** if an organisation containing your details suffers a **data breach**. Criminals will use these stolen customer details (such as user names and passwords) to try and access other systems and accounts.

Create strong passwords

Create a strong and memorable password for your email account (and other important accounts).

Avoid using predictable passwords (such as **dates, family** and **pet names**). Avoid the most common passwords that criminals can easily guess (like 'passw0rd').

Don't re-use the same password across important accounts. If one of your passwords is stolen, you don't want the criminal to also get access to (for example) your banking account.

To create a **memorable password** that's also hard for someone else to guess, you can **combine three random words** to create a single password (for example cupfishbiro).

Look after your passwords

If you store your passwords somewhere safe, you won't have to remember them. This allows you to use unique, strong passwords for all your important accounts.

You can write your password down to remember it, but **keep it somewhere safe**, out of sight, and (most importantly) **away from your computer**.

Store your passwords in your browser when prompted; it's quick, convenient and safer than re-using the same password. Browsers can also detect 'dodgy' websites that phishing emails try and trick you into visiting.

You can also use a standalone **password manager** app to help you create and store strong passwords.

Use 2FA to protect your account

Many companies allow you to set up two-factor authentication (also known as 2FA) on your accounts. It's called 2FA because it involves signing into your account using **two passwords or codes;** one that you know, and the other usually sent to your phone.

The most common form of 2FA is when a code is sent to your smartphone that you must enter in order to proceed. You should **set up 2FA for important websites** like banking and email.

Even if a criminal knows your passwords, they will struggle to access any accounts that you've protected by turning on 2FA.

Visit **www.ncsc.gov.uk/2fa** for up-to-date instructions on how to set up 2FA across popular online services such as Gmail, Facebook, Twitter, LinkedIn, Outlook and Instagram.

What to do if your password is stolen?

If you suspect your password has been stolen, you should change it as soon as possible.

If you have used the same password on any other accounts, change these as well.

You can use the website **www.haveibeenpwned.com** to check if your information has ever been made public in a major data breach.

NCSC Password Tips

National Cyber Security Centre

Password Policy
Advice for system owners

The NCSC is working to reduce organisations' reliance on users having to recall large numbers of complex passwords. The advice below advocates a greater reliance on technical defences and organisational processes, with passwords forming just one part of your wider access control and identity management approach.

How passwords are discovered...

Interception
Passwords can be intercepted as they travel over a network.

Brute force
Automated guessing of billions of passwords until the correct one is found.

Key logging
Installing a keylogger to intercept passwords when they are entered.

Manual guessing
Details such as dates of birth or pet names can be used to guess passwords.

Shoulder surfing
Observing someone typing in their password.

Stealing passwords
Insecurely stored passwords can be stolen, such as ones written on sticky notes and kept near (or on) devices.

Stealing hashes
Stolen hash files can be broken to recover the original passwords.

Phishing & coercion
Using social engineering techniques to trick people into revealing passwords.

Data breaches
Using the passwords leaked from data breaches to attack other systems.

Password spraying
Trying a small number of commonly-used passwords to access a large number of accounts.

...and how to improve system security.

Reduce your reliance on passwords

1. Only use passwords where they are needed and appropriate.
2. Consider alternatives to passwords such as SSO, hardware tokens and biometric solutions.
3. Use MFA for all important accounts and internet-facing systems.

Implement technical solutions

1. Throttling or account lockout can defend against brute force attacks.
2. For lockout, allow between 5-10 login attempts before locking out.
3. Consider using security monitoring to defend against brute force attacks.
4. Password blacklisting prevents common passwords being used.

Protect all passwords

1. Ensure corporate web apps requiring authentication use HTTPS.
2. Protect any access management systems you manage.
3. Chose services and products that protect passwords using standards such as SHA-256.
4. Protect access to user databases.
5. Prioritise administrators, cloud accounts and remote users.

Help users generate better passwords

1. Be aware of different password generation methods.
2. Use built-in password generators when using password managers.
3. Don't use complexity requirements.
4. Avoid the creation of passwords that are too short.
5. Don't impose artificial capping on password length.

Key messages for staff training

1. Emphasise the risks of re-using passwords across work and home accounts.
2. Help users to choose passwords that are difficult to guess.
3. Help users to prioritise their high value accounts.
4. Consider making your training applicable to users' personal lives.

Help users cope with password overload

1. Allow users to securely store their passwords, including the use of password managers.
2. Don't automatically expire passwords. Only ask users to change their passwords on indication or suspicion of compromise.
3. Use delegation tools instead of password sharing. If there's a pressing business requirement for password sharing, use additional controls to provide the required oversight.

www.ncsc.gov.uk @ncsc National Cyber Security Centre

https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

Multi-factor authentication

- Menti

1. What is multi-factor authentication?
2. Give an example of multi-factor authentication and identify what the factors are?

Size *is* important

Length (chars)	Number of permutations		
	Alphabetic	Alphanumeric	Alphanumeric + ten other symbols
1	26	36	46
2	676	1,296	2,116
3	17,576	46,656	97,336
4	456,976	1,679,616	4,477,456
5	11,881,376	60,466,176	205,962,976
6	308,915,776	2,176,782,336	9,474,296,896
7	8,031,810,176	78,364,164,096	435,817,657,216
8	208,827,064,576	2,821,109,907,456	20,047,612,231,936
9	5,429,503,678,976	101,559,956,668,416	922,190,162,669,056
10	141,167,095,653,376	3,656,158,440,062,980	42,420,747,482,776,600

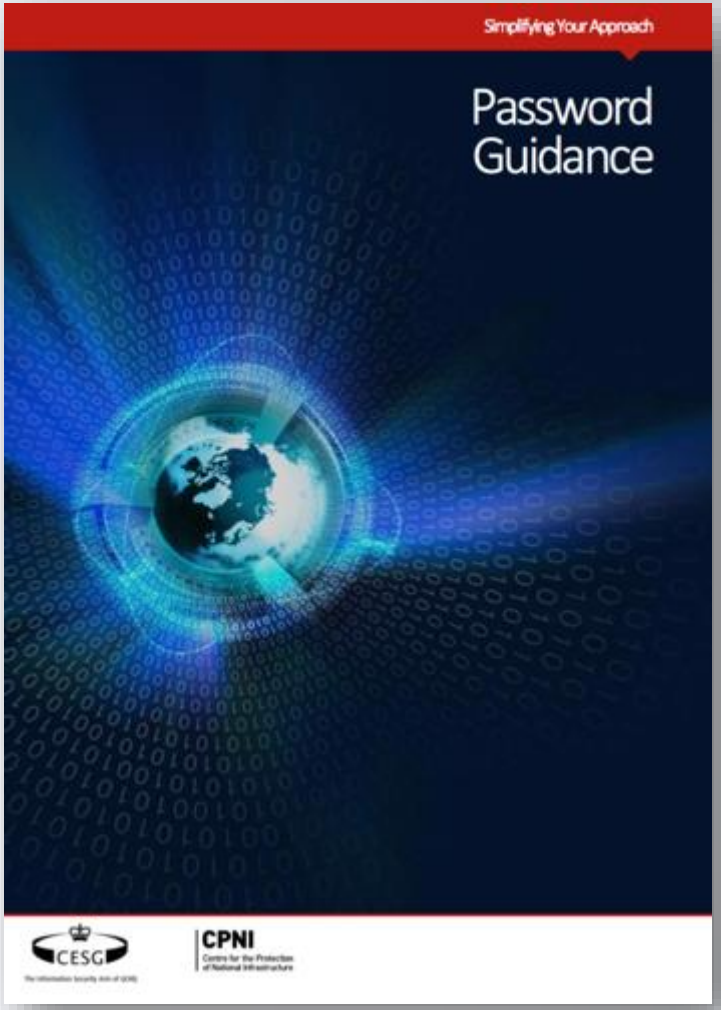
Improving Password Systems

- Encourage better selection
- Password ageing
- Password filtering
- Prevention of password reuse
- System generated passwords
- One-time passwords

Decreases user-friendliness?

Challenging conventions

- 2015 CESG guidance explicitly advices *against* the practice of forcing regular password change
- Recognises the usability challenge for users
  - more likely to write it down or incur helpdesk support for forgotten passwords
- Advises other safeguards to compensate, such as showing last login time to alert users to compromise



https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

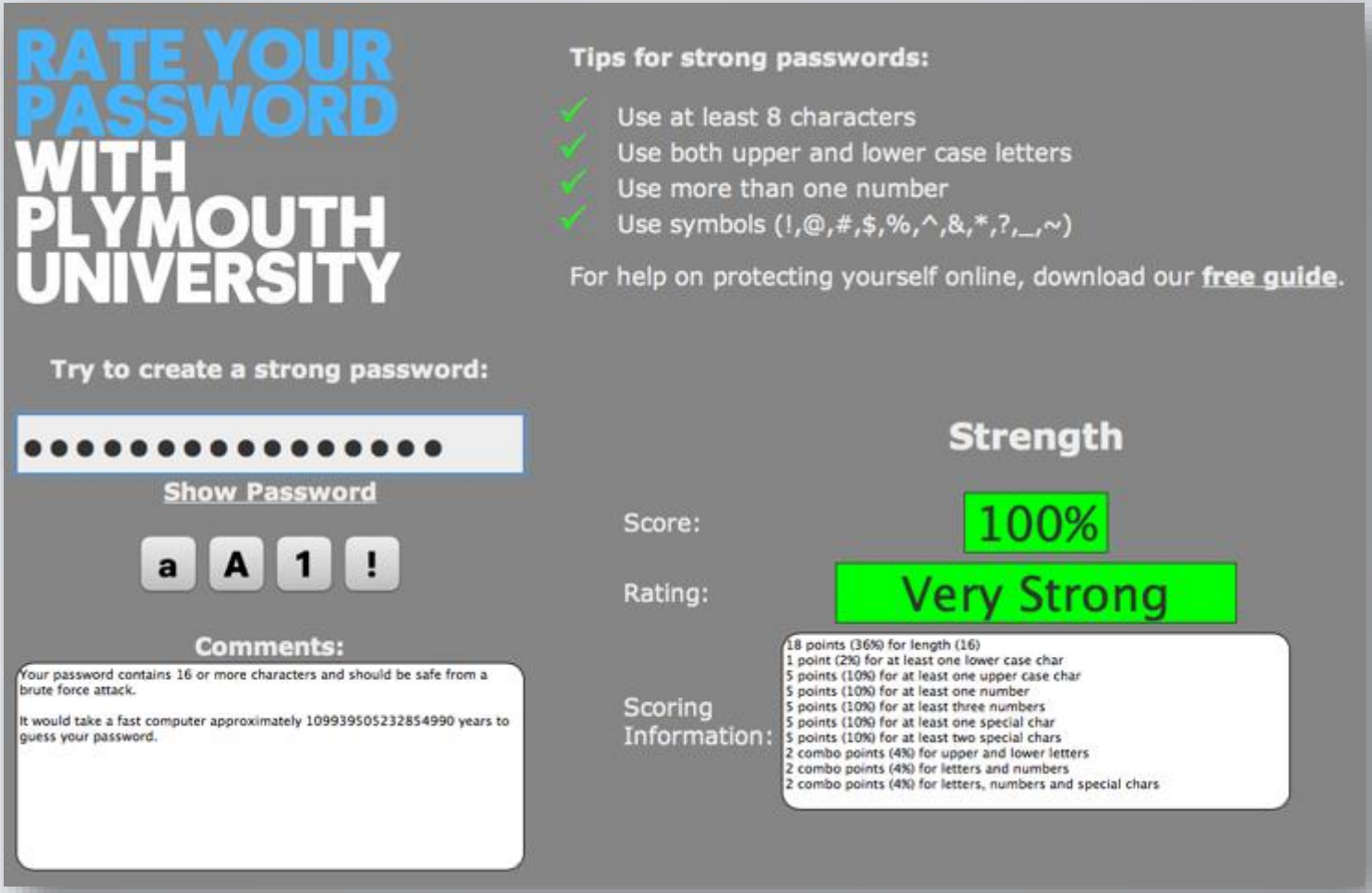
Usability challenges

- Practically every aspect of good password practice makes them more difficult to use
  - Enforcing selection criteria (length and character composition)
  - Changing them regularly
  - Avoiding password reuse
  - Avoiding a written record
- The need to use passwords across multiple systems amplifies the challenge
- Password management tools overcome some of the constraints but complicate the process of retrieving and using the passwords

The Security Disconnect?
Password protection

- What we are *told*
  - Your password is too weak
- What we want to *know*:
  - Why is it weak?
  - How can we make it better?
  - Why does it matter?

If you want to play . . .



www.cscan.org/passwordstrength/

And another one . . .

password.kaspersky.com

Password advice

- 3-4 students per group, 10 mins

Scenario: Alice has many online accounts: university student account, Netflix, Amazon, BBC iplayer, online accounts of 2 different banks, youtube, facebook, a personal email and a few accounts of different shopping companies like gooutdoors, a few game websites. At home she has a desktop which is shared among her family members, a personal laptop which is only used by her. Most of the time she uses her personal laptop, but sometimes she uses the desktop. When she goes to the university, she uses the university computers to access the university services.

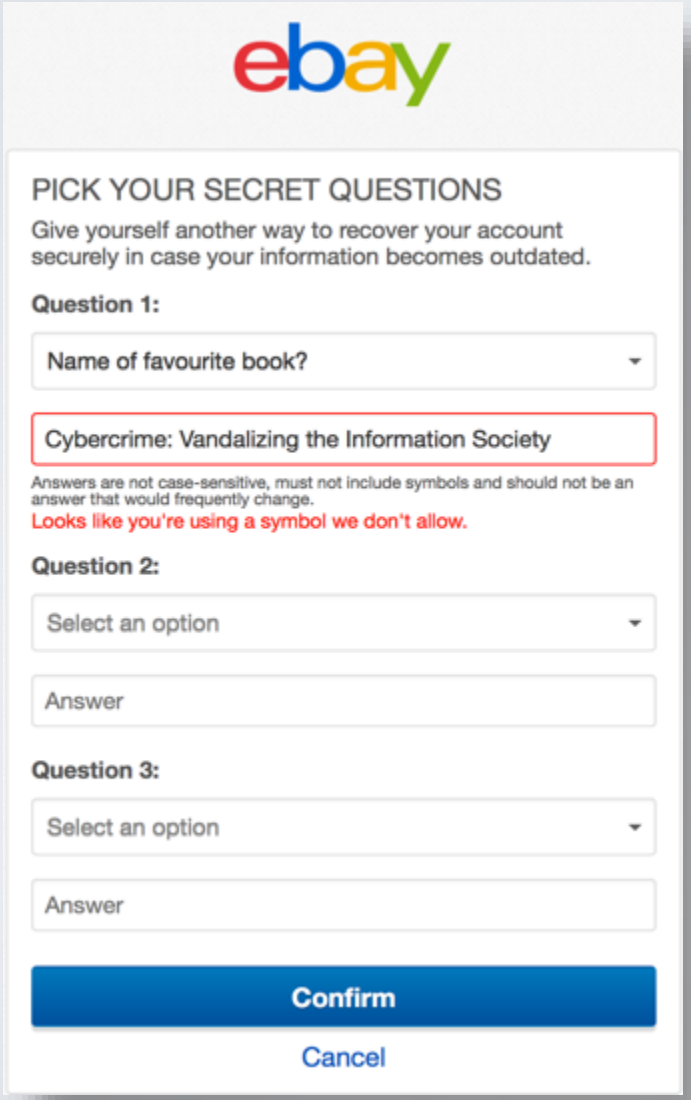
Your task is to devise a strategy/ good practices/ advice of creating, storing and using passwords for Alice. Details would be necessary.

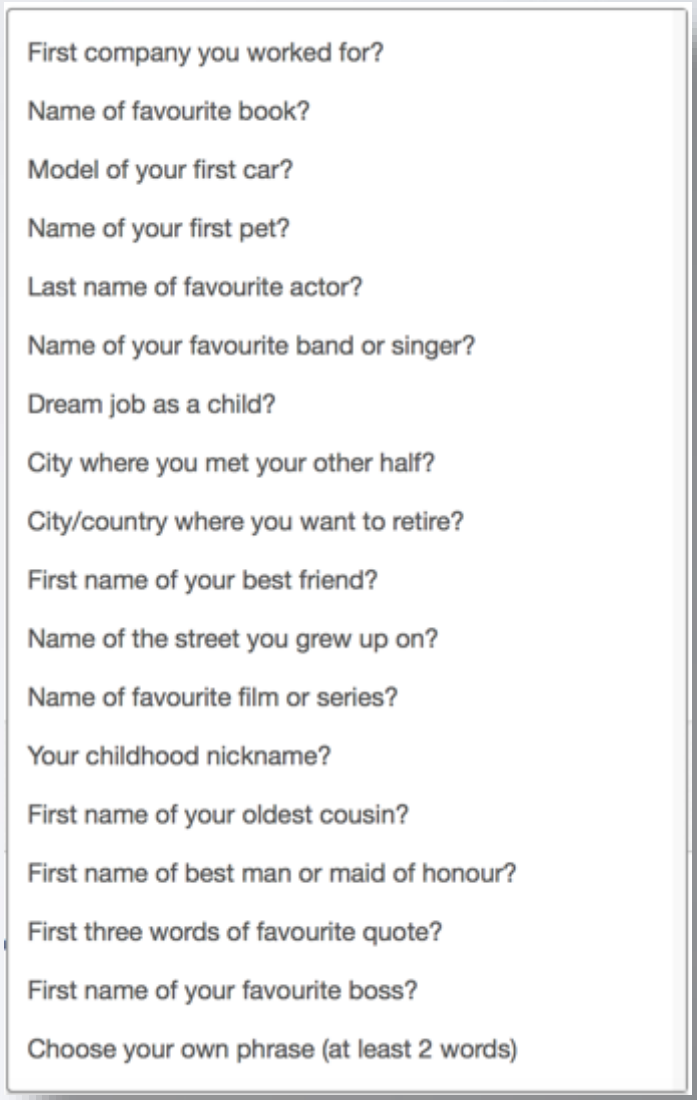
Write your group strategy/ advice

Question and Answer methods

- User must correctly answer one or more questions in order to verify their identity
  - Hold a repository of questions and then randomly select a subset at each login
- Questions must require answers that:
  - are suitably tied to the legitimate user (to prevent everyone having similar answers)
  - are not easy to discover or guess
- Often used to verify identity when the user has forgotten their password, rather than as the primary authentication method

Cognitive challenges





The challenges of cognitive challenges

- The list included a mix of factual and opinion-based questions.
  - factual questions (e.g. “What street did you grow up on?”) could be more reliable
  - opinions (e.g. “What is your favourite pastime?”) may change and cause users to provide incorrect responses if they do not remember (or update) their original answers
- Need to offer questions that all users should be able to answer
  - e.g. some users may not have had a pet, school mascot, car, bike or spouse

The challenges of cognitive challenges

- Allow users to compose their own questions?
  - runs the risk of them taking a similarly cavalier approach to that when selecting passwords (i.e. choosing questions to which others may also know the answers)
- Preferable to have a large set of well-chosen, preset questions, and allow the user to select a subset of these at enrolment
- Could still be vulnerable to an impostor with intimate knowledge of the user and their background

Graphical / image-based methods

- The theoretical basis is that images are easier to remember than strings of characters
- Methods that *present* images (rather than requiring users to draw them) enable *recognition* rather than precise *recall* as the basis for authentication
  - a skill that people have shown to be better at performing
- Positive findings in terms of users' ability to remember the required information *and* their acceptance of the methods in practice
  - albeit with the majority of approaches coming from the research community, and not widely evaluated

Graphical alternatives

- Remembering a *sequence* of images
  - *Déjà Vu* requires users to remember a series of photos or abstract images
  - *PassImages* uses pictures of everyday items
  - *Passfaces* relies upon recognition of a series of faces
  - *DynaHand* relies upon users' ability to recognize pictures of their own signature
- Remembering *something about* an image
  - e.g. areas or points within a picture (e.g. *PixelPin*)
- Requiring the user to *draw* an image
  - e.g. Jermyn et al. (1999) presented a method in which the 'password' was realized as a simple picture drawn on a grid

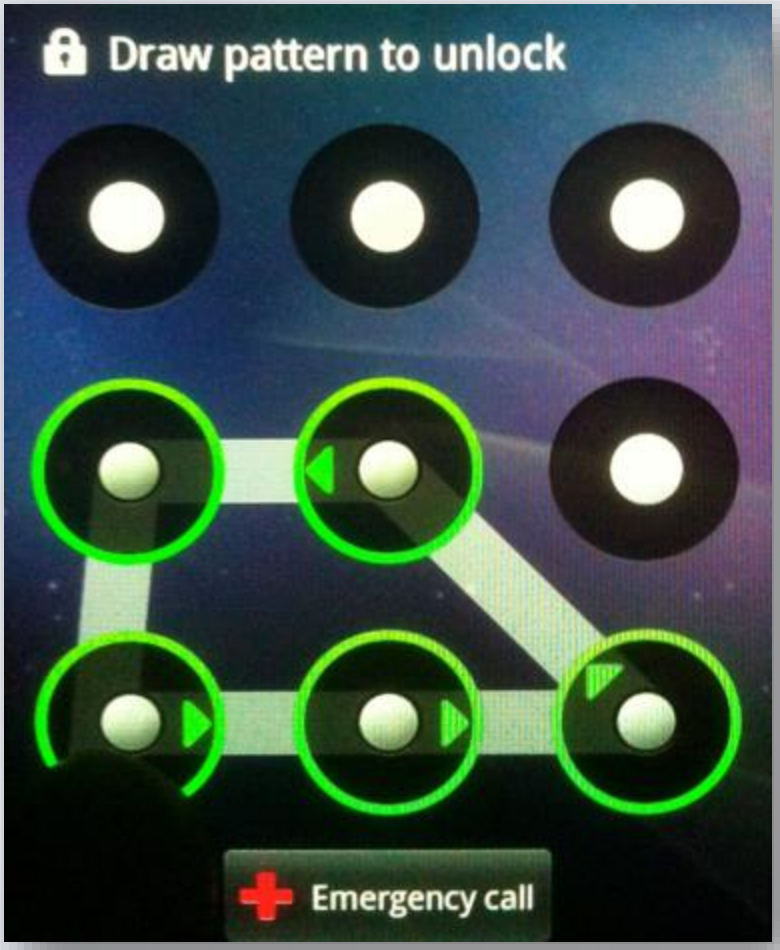
An image-based example

GOTPass (2015)

- Replacing weak password and PIN-based authentication
- A method based upon remembering pictures of objects
- Listed in TechRepublic's "*10 of the latest security products that can help you fight the bad guys*" (Feb 2016)

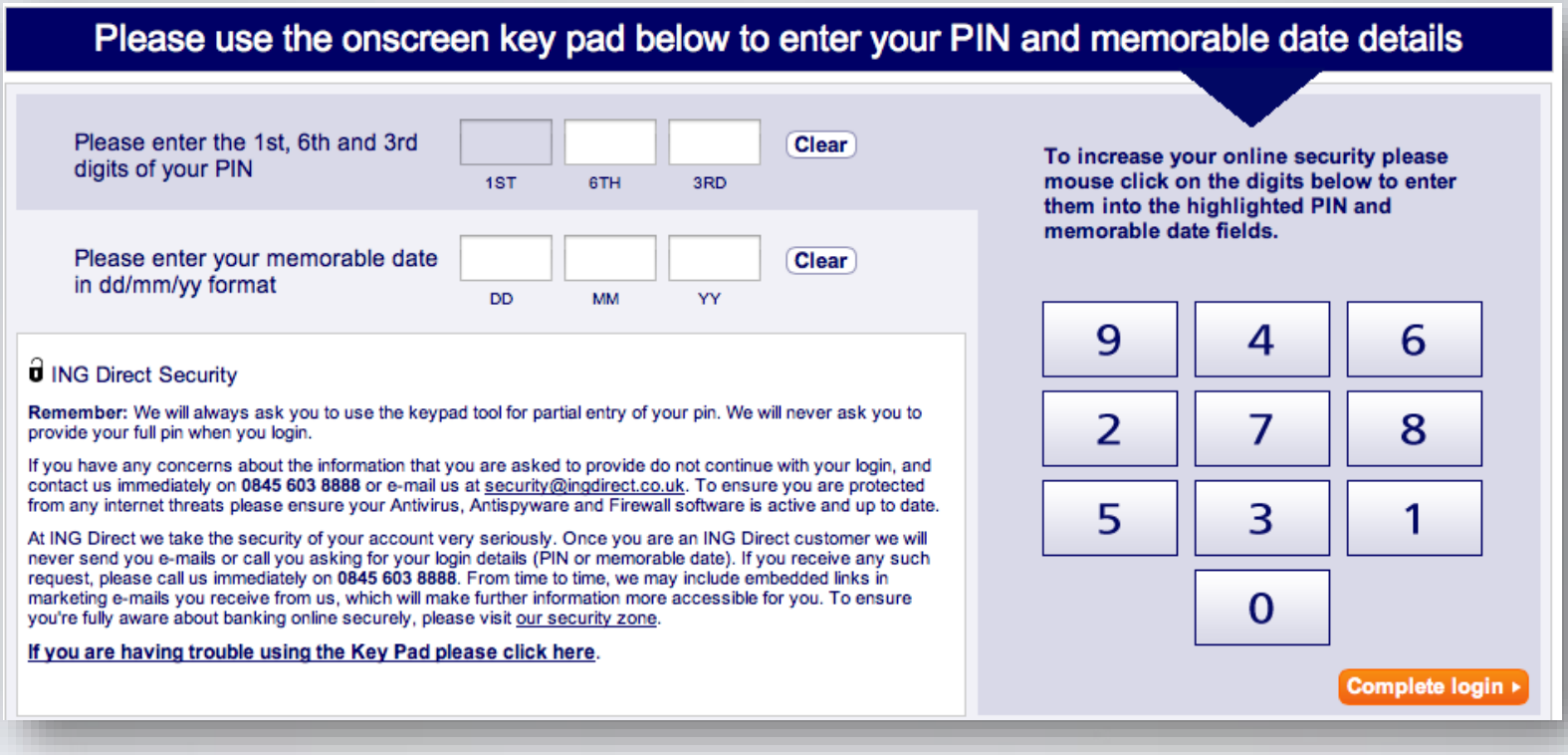
Windows Picture Password

Android Pattern Unlock



- Clearly suited to touch screen devices
- Complex patterns hard to remember?
- More observable than PINs
- Potential clues from greasy fingers
  - choose patterns that double-back …
  - … or clean the screen!

Online Banking



- Identification and authentication demands:
  - A personal banking number
  - Customer surname
  - Selected digits from security number
  - A memorable date

Challenging the legitimate user?

- More time-consuming and require more cognitive effort than passwords:
  - the authentication challenge will not be the same each time (i.e. different digits requested)
  - the user can no longer rely on reflex response of typing a normal PIN/password
  - the digits of the PIN are not requested in sequential order
  - the position of the digits on the graphical keypad varies on each occasion

Comparison factors

- Mental effort
  - the extent to which the technique relies upon the user's ability to memorise and recall things, and how precise this must be
- Convenience
  - e.g. as the speed with which the user is able to login, and the effort/engagement required to do so
- Applicability
  - e.g. whether the technique will work effectively on desktop, mobile and handheld devices, with differing input mechanisms and screen sizes/resolutions
- Flexibility
  - e.g. the ease with which the user can change their authentication credentials in the event of compromise

Comparison authentication approaches

Menti, individidual

1. Search for the scientific paper using Google Scholar (with instruction): Are Passfaces more usable than passwords
2. Skim the paper to answer the following question:

Compared to password-based authentication, what are its pros/ cons in mental effort, convenience, applicability or flexibility?

3. Write on menti

Password requires more mental effort than passfaces, for instance, users need more help to remind the password [1]

Reference:

1. Brostoff, Sacha, and M. Angela Sasse. "Are Passfaces more usable than passwords? A field trial investigation." *People and computers XIV—usability or else! Proceedings of HCI 2000*. Springer London, 2000.

Token-based authentication

Token-based Authentication

- Based upon possession of a physical identifier
- Examples:
  - Magnetic cards
  - Smart cards (e.g. Chip and PIN)
  - Code generators (e.g. RSA SecurID)
  - Radio transmitter devices (e.g. RFID)
- Often combined with secret knowledge to form a 2-stage authentication (and 2-factor authentication)

Which is 2-stage authentication (2-step authentication)

a. User is authenticated using password and security questions
b. User is authenticated using ATM card and PIN

Which is 2FA (2-factor authentication)

a. User is authenticated using password and security questions
b. User is authenticated using ATM card and PIN

Token-based Authentication

- *Advantages*
  - Avoids masquerade potential of passwords
  - Users cannot (easily) share their access privileges
  - Increased awareness of likely compromise
  - An attacker must counterfeit or steal a token before gaining access
  - Illegal possession of a token can be used as evidence of an attempt to gain unauthorised access

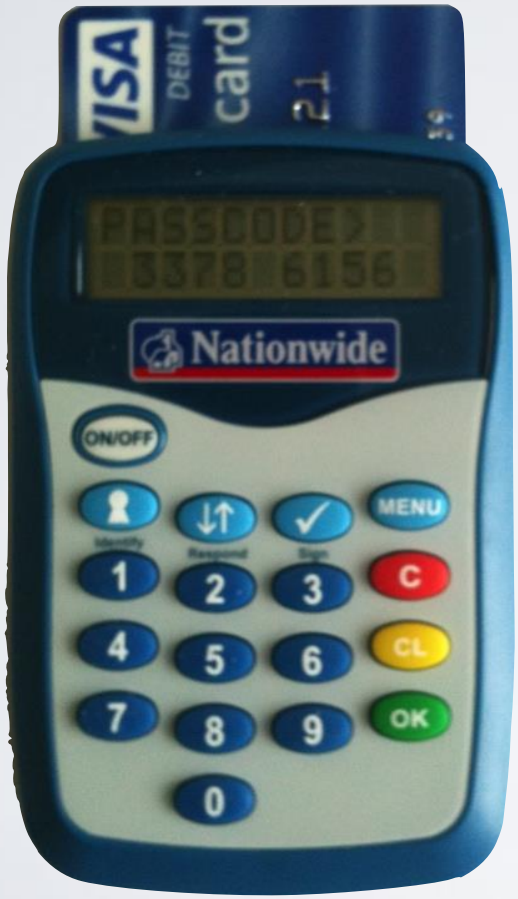
Token-based Authentication

- *Disadvantages*
  - More expensive to implement (esp. large scale)
  - Tokens can still be lost or stolen
  - Combining with secret knowledge reintroduces some of the disadvantages of that approach

Online Banking

Codes and Cards

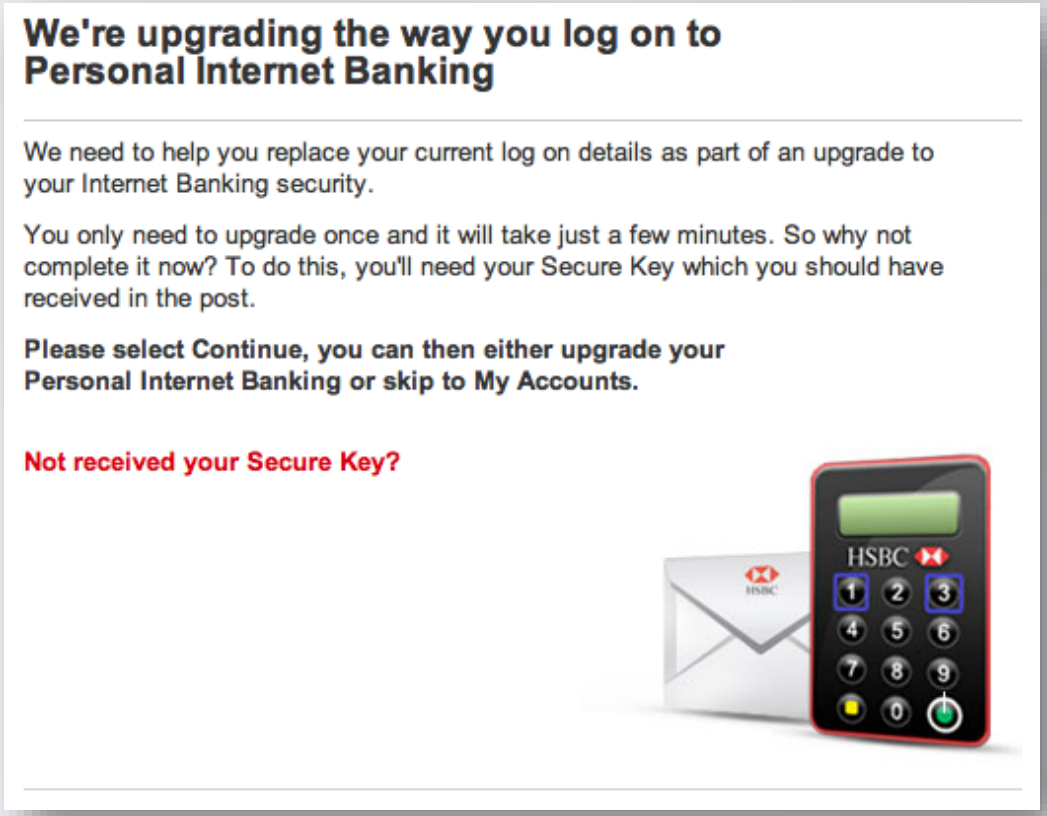
Online Banking
Card readers



- User places their banking card into the reader
- Authenticates using the card's PIN
- Receives a pass code for other operations
- Examples from Barclays (PIN Sentry), Nationwide, NatWest …

Online Banking
HSBC Secure Key

- Identification and authentication demands:
  - A personal banking number
  - The Secure Key token and its accompanying PIN
  - An answer to a secret question

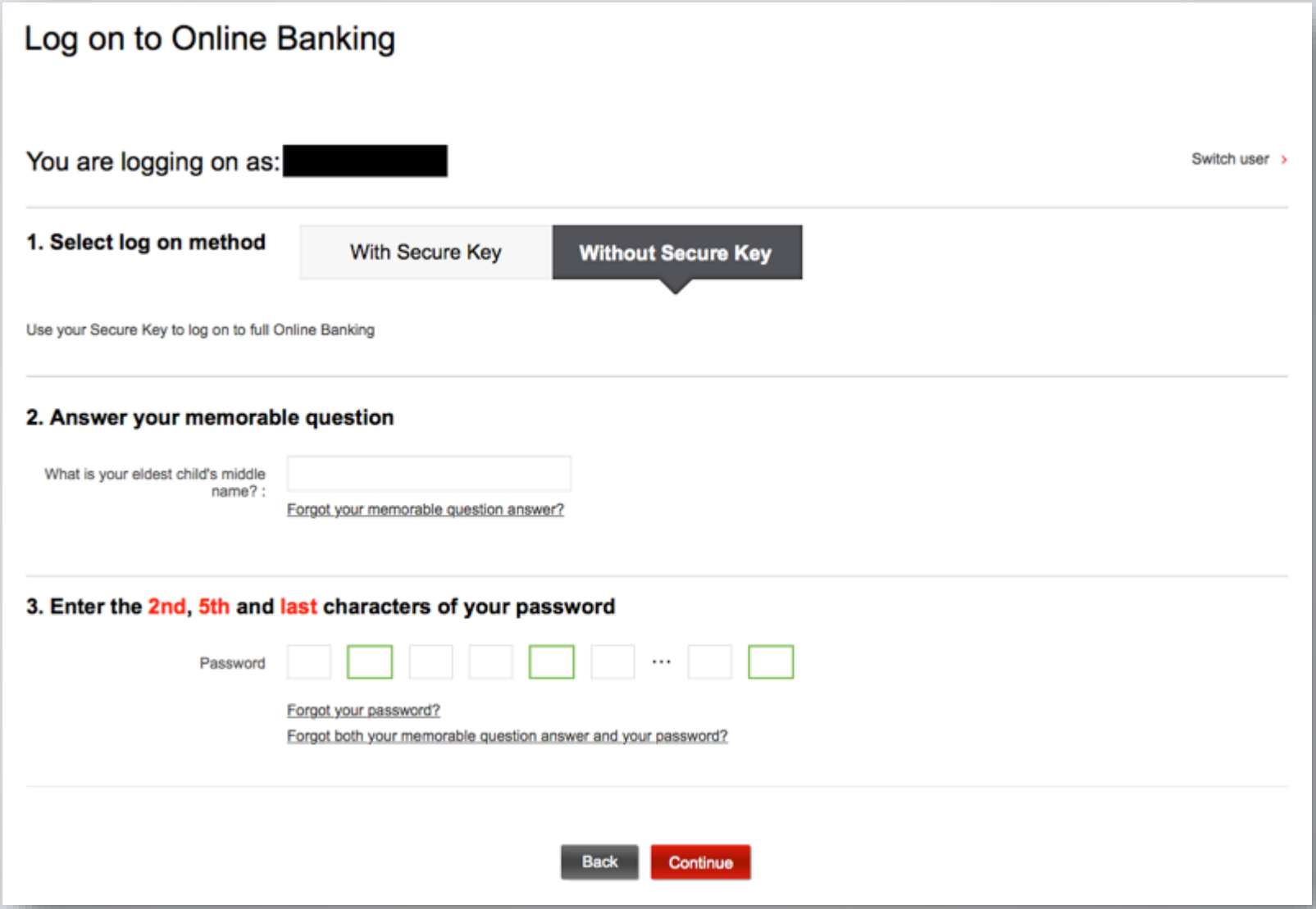


The Secure Key login process

- HSBC Secure Key introduces a **multi-stage process** for each login:
  - User needs to enter their Banking ID
  - Then answer a security question defined when they set up the account
  - Then enter a 4-digit PIN code on the Secure Key device
  - Then enter the 6-digit code generated by the device into the web page

Differentiated Authentication

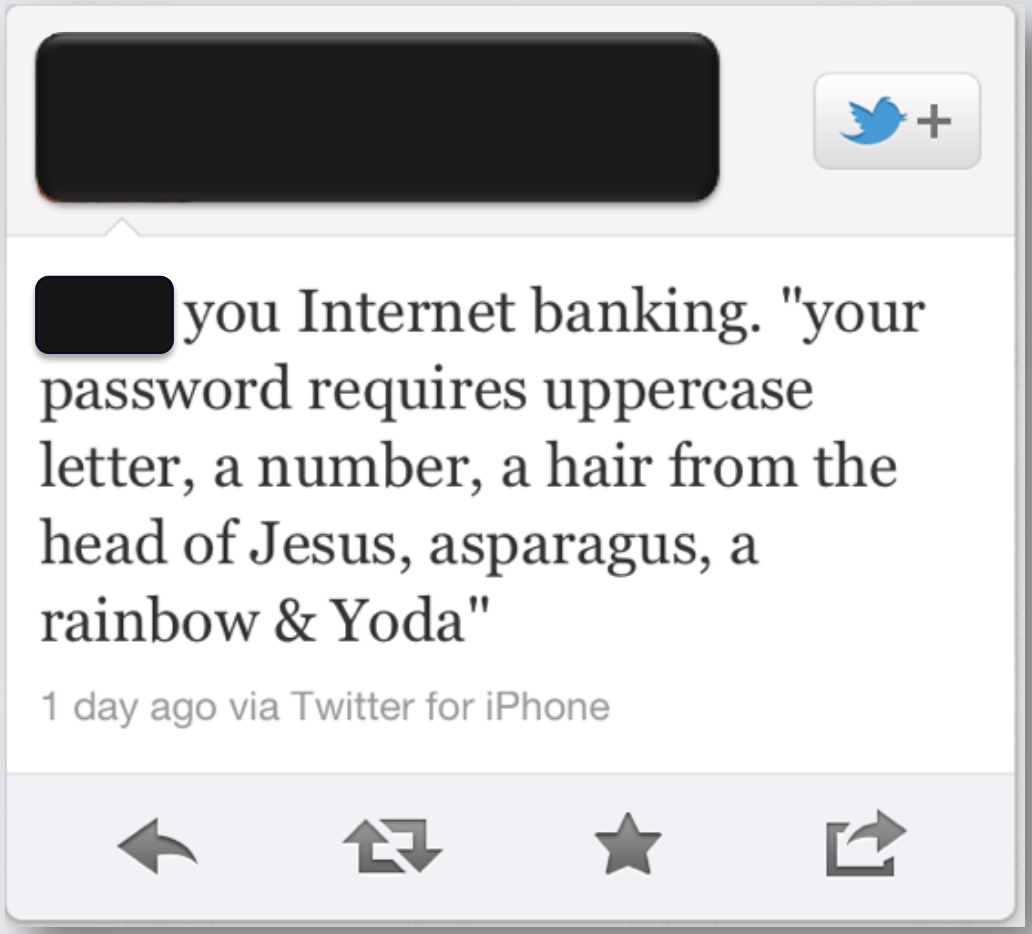
(Choice added in 2015)



Acceptable trade-off?

- Users may not object in a banking context
  - they realise their money is at stake
- Such approaches would not work for website authentication in general
  - would not scale up well as having a variety of numbers to remember for different accounts would quickly become unmanageable for the user

The user's viewpoint?



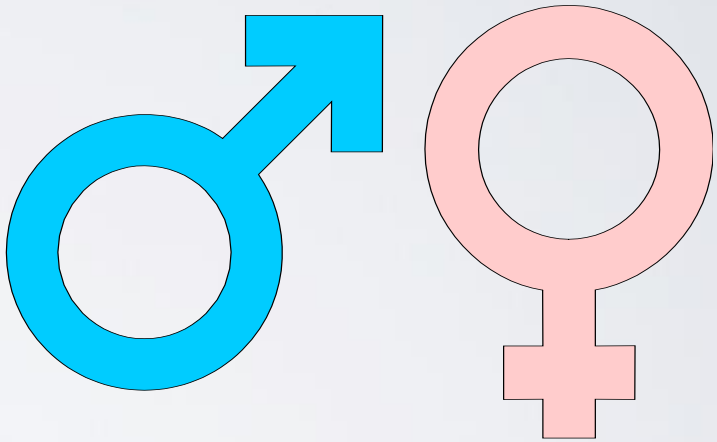
Biometrics

Activity

- Which biometrics information can be used for authentication?

Biometrics

- Authentication based upon something the user *is*
- Theoretically far more usable
  - nothing for the user to remember
  - nothing to them to lose or leave behind
- Practical factors (e.g. failure to acquire, false rejection) may limit tolerability



Biometrics
Some definitions

As a *characteristic*:

"A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition”

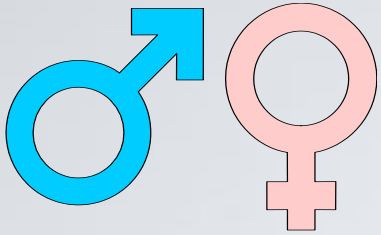
As a *process*:

“The automated use of physiological or behavioral characteristics to determine or verify identity”

Newbold's Biometric Dictionary (2007)

Desirable Attributes

- **Uniqueness** - the ability to successfully discriminate people
- **Universal** - the ability for a technique to be applied to a whole population of users
- **Permanence** - the ability for the characteristics not to change with time.
- **Collectable** - the ease with which a sensor is able to collect the sample
- **Acceptable** - the degree to which the technique is found to be acceptable by a person
- **Circumventable** - the ability not to duplicate or copy a sample



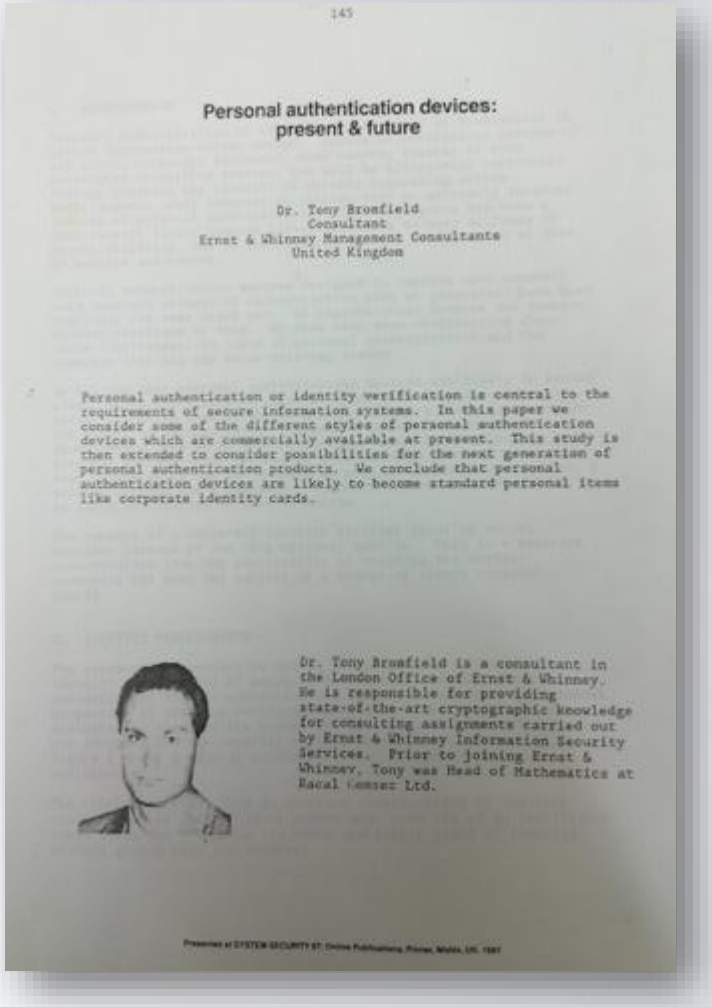
Biometric Approaches

Physiological	Behavioural
Fingerprint Recognition	Speaker Recognition
Hand Geometry	Signature Recognition
Vascular Pattern Recognition	Keystroke Analysis
Iris Scanning	Mouse Dynamics
Retinal Scanning	Gait Recognition
Facial Recognition	Stylometry
Facial Thermogram	
Ear print	

Biometrics
A long-predicted revolution?

"We expect that personal authentication devices will become commonplace within five years and that biometric identification methods will complement these devices rather than replace them"

Ernst & Whinney
Management Consultants, 1987



145

Personal authentication devices:
present & future

Dr. Tony Bromfield
Consultant
Ernst & Whinney Management Consultants
United Kingdom

Personal authentication or identity verification is central to the requirements of secure information systems. In this paper we consider some of the different styles of personal authentication devices which are commercially available at present. This study is then extended to consider possibilities for the next generation of personal authentication products. We conclude that personal authentication devices are likely to become standard personal items like corporate identity cards.

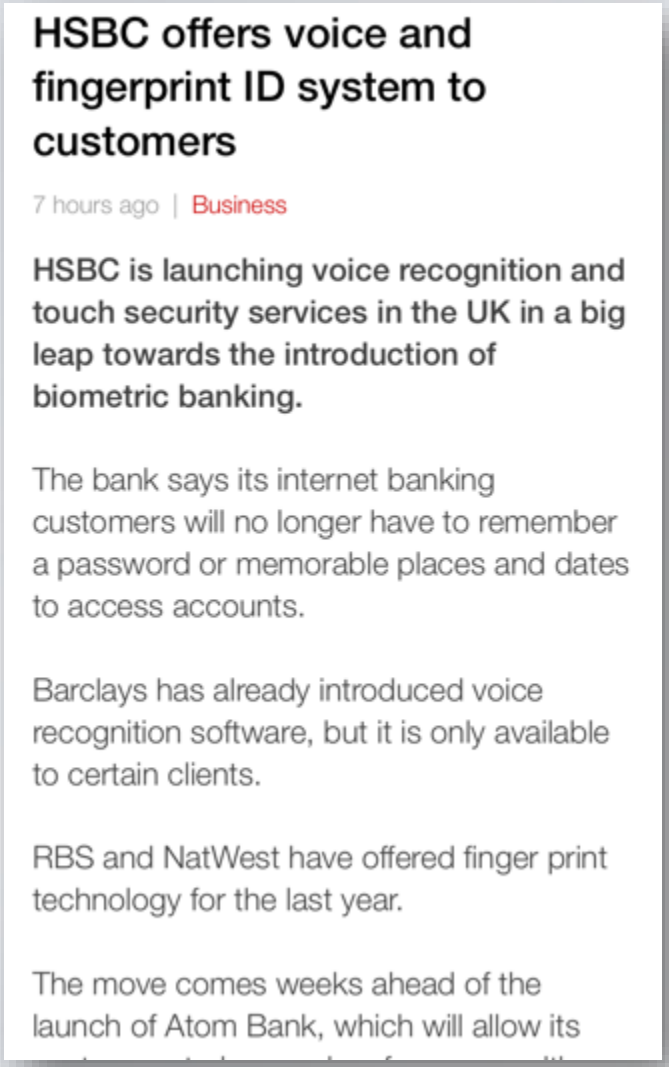
Dr. Tony Bromfield is a consultant in the London Office of Ernst & Whinney. He is responsible for providing state-of-the-art cryptographic knowledge for consulting assignments carried out by Ernst & Whinney Information Security Services. Prior to joining Ernst & Whinney, Tony was Head of Mathematics at Racal Comsec Ltd.

In the past . . .

"*Finger and iris scanning as well as voice recognition and dynamic signature have all been put forward as possibilities. Such technology, however,* ***is not sufficiently reliable*** *or cost-effective in a point-of-sale environment to meet the requirements of the UK card industry* ***within the next ten years***."

Card Fraud 2005 – The Facts
Association for Payment Clearing Services (APACS)
April 2005

~10 years later . . .



HSBC offers voice and fingerprint ID system to customers

7 hours ago | Business

HSBC is launching voice recognition and touch security services in the UK in a big leap towards the introduction of biometric banking.

The bank says its internet banking customers will no longer have to remember a password or memorable places and dates to access accounts.

Barclays has already introduced voice recognition software, but it is only available to certain clients.

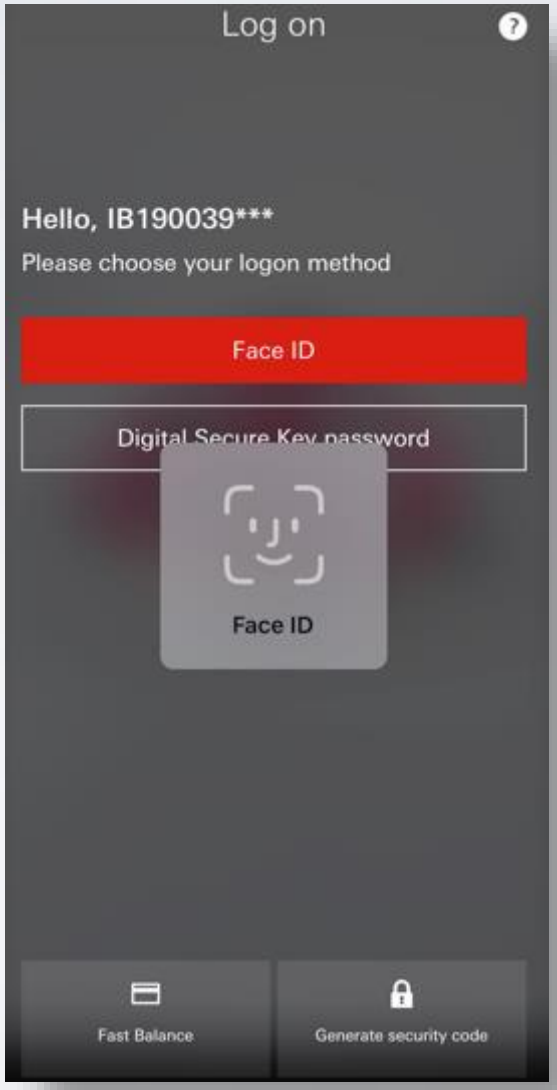
RBS and NatWest have offered finger print technology for the last year.

The move comes weeks ahead of the launch of Atom Bank, which will allow its

- Banks are backing biometrics
- Survey of 2,038 people, commissioned by HSBC
  - 55% rarely changed passwords
  - 74% felt that biometric security would become the default "password" of the future

BBC News
19 February 2016
http://www.bbc.co.uk/news/business-35609833

In the present . . .

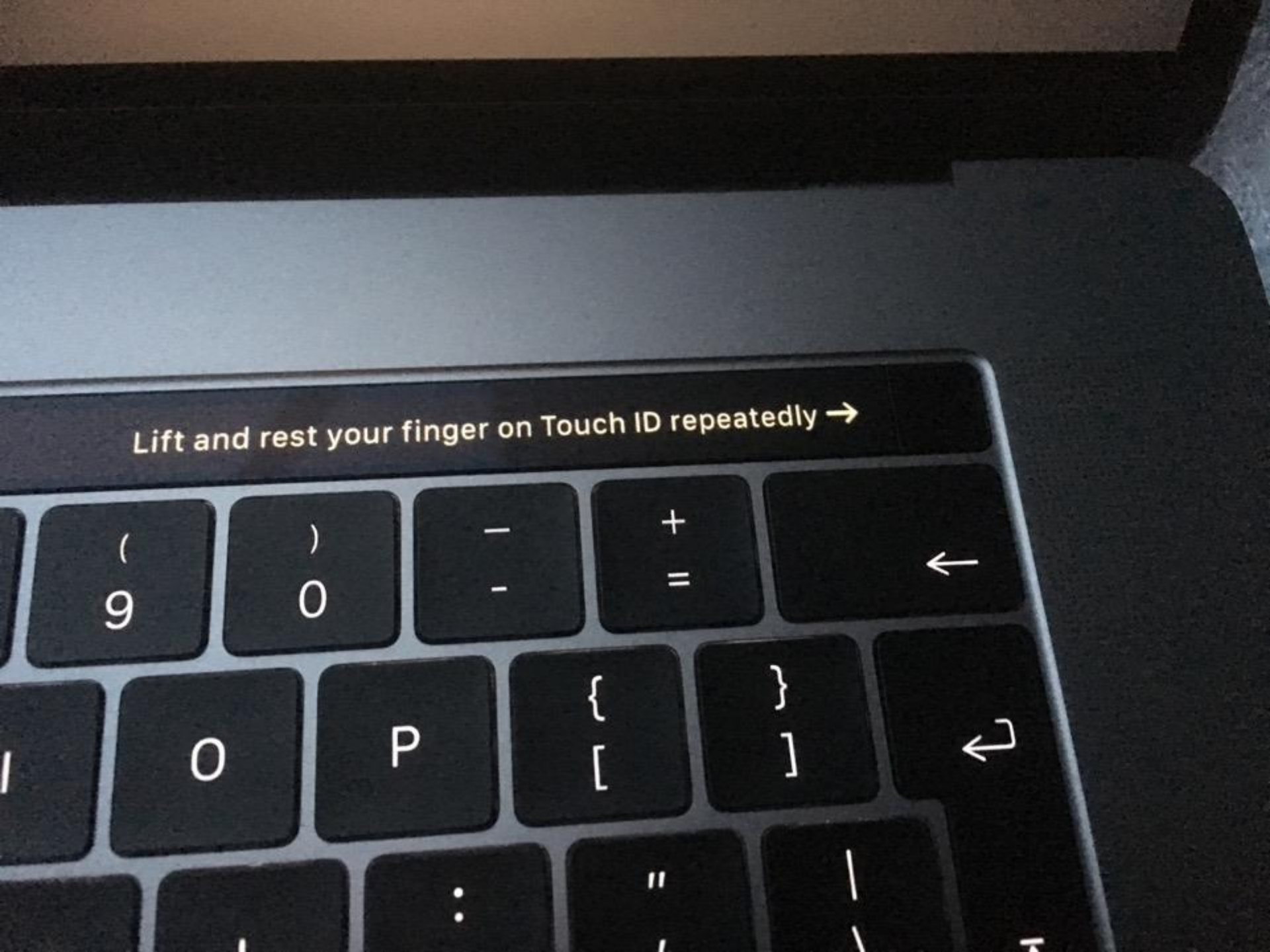


HSBC Mobile Banking app
February 2018

Biometrics in the past

HP iPAQ H5450 (2002)
and later models

Biometrics today

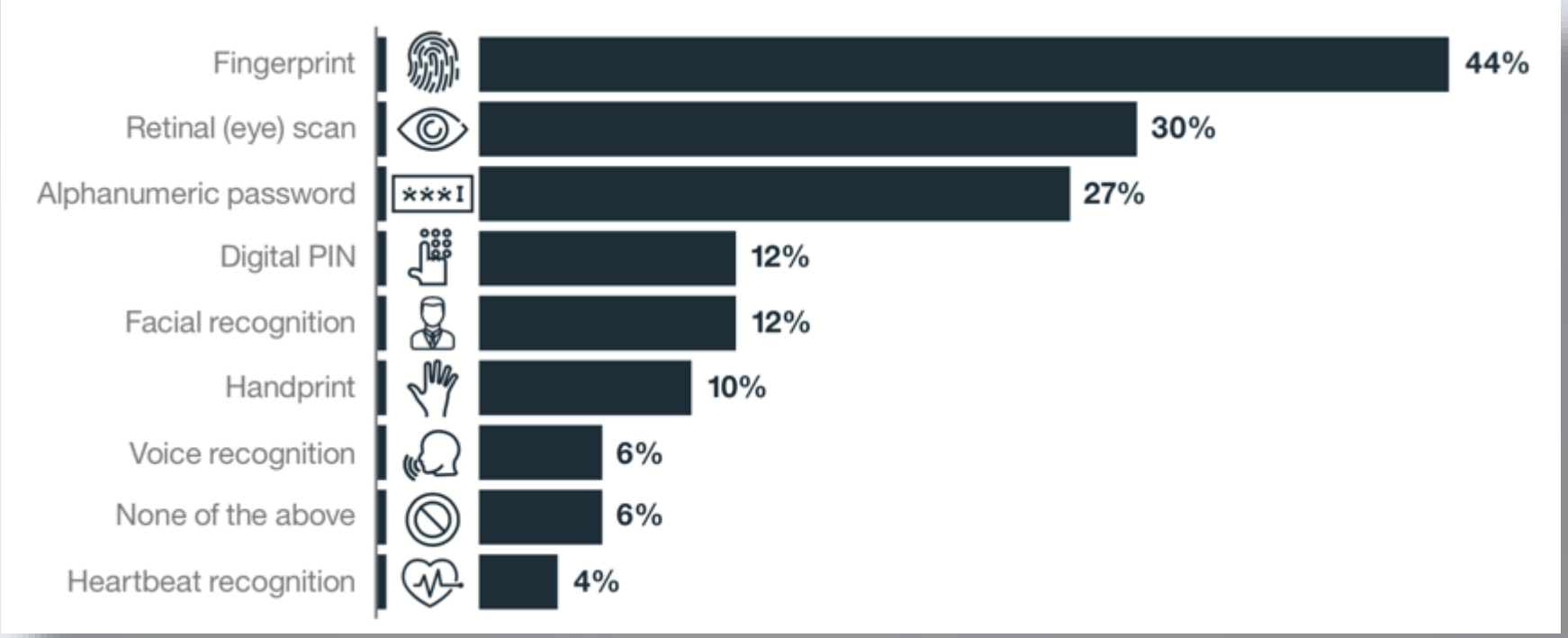

Lift and rest your finger on Touch ID repeatedly →
(9
) 0
– -
+ =
O
P
{ [
}]
: ;
" '
| \

The Rise of Biometrics

- Key rationale is ease of use
  - a (correctly used) password can deliver security but becomes increasingly impractical
  - we need usable alternatives
- Most prominent growth has been on mobile devices
  - driven by increasing need to protect them and disinclination to use passcodes
  - integrating biometrics makes the process easier and quicker

Perceived Protection

Authentication methods perceived as the most secure



67% are comfortable using biometrics today

(based on 3,977 adults across the United States, European Union and Asia-Pacific regions)

IBM Security: Future of Identity Study
January 2018

Analyze fingerprints-based authentication

Ref: https://www.ncsc.gov.uk/collection/biometrics

1. What are the cons?
2. What are the pros?

Fingerprints-based authentication pros & cons

- Pros:
  - Mental effort: users do not need to remember, they never forget
  - Convenience: little effort from the user, high acceptance from users
  - Security: cannot easily share, person need to be present for authentication
- Cons:
  - Mental effort: need knowledge and user experience
  - Convenience: false reject, false match can happen (accuracy issues)
  - Applicability: work on phone/ laptop with sensors, do not work on computers without sensors
  - Flexibility: if compromised, change is limited
  - Price: more expensive than passwords

Fingerprint Failings?

- There are some circumstances in which Touch ID stops working
- Notable cases:
  - Moisture
    - Sweaty hands
    - Rain!
  - Dirty fingers
  - Gloves
  - Skin damage

Error Rates and Operational Factors

- **False Acceptance Rate** (FAR)
  - Errors where impostors are falsely believed to be legitimate users
- **False Rejection Rate** (FRR)
  - Errors where the system falsely identifies the legitimate user as an impostor
- **Failure to Enroll**
  - Errors in which the system is unable to establish a biometric template for a proposed user
- **Failure to Acquire**
  - Errors in which the system is unable to successfully acquire the information required to make a decision

- A legitimate user's experience of biometrics will be informed by:
  - combined False Rejection and Failure to Acquire rates
  - the throughput of the system

Compare biometrics-based system using FAR/ FRR

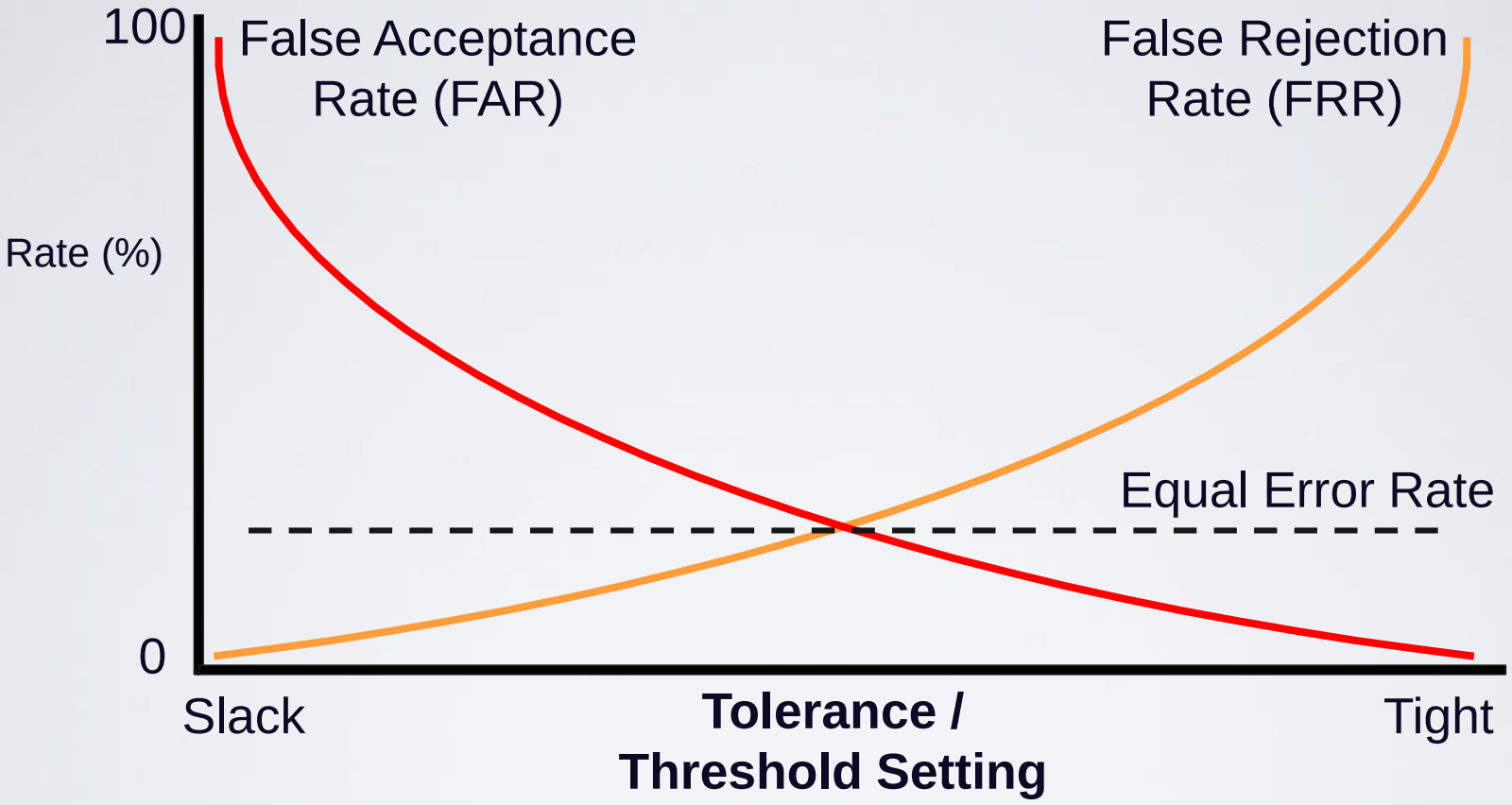
- Menti
- Given the following two fingerprint authentication systems with their FAR, FRR values

a. FRR = 7.5% and FAR = 0.1%
b. FRR = 6% and FAR = 0.2%

Which system is more secure?

Which system is more convenient?

FAR / FRR relationship



Simplified biometric matching model

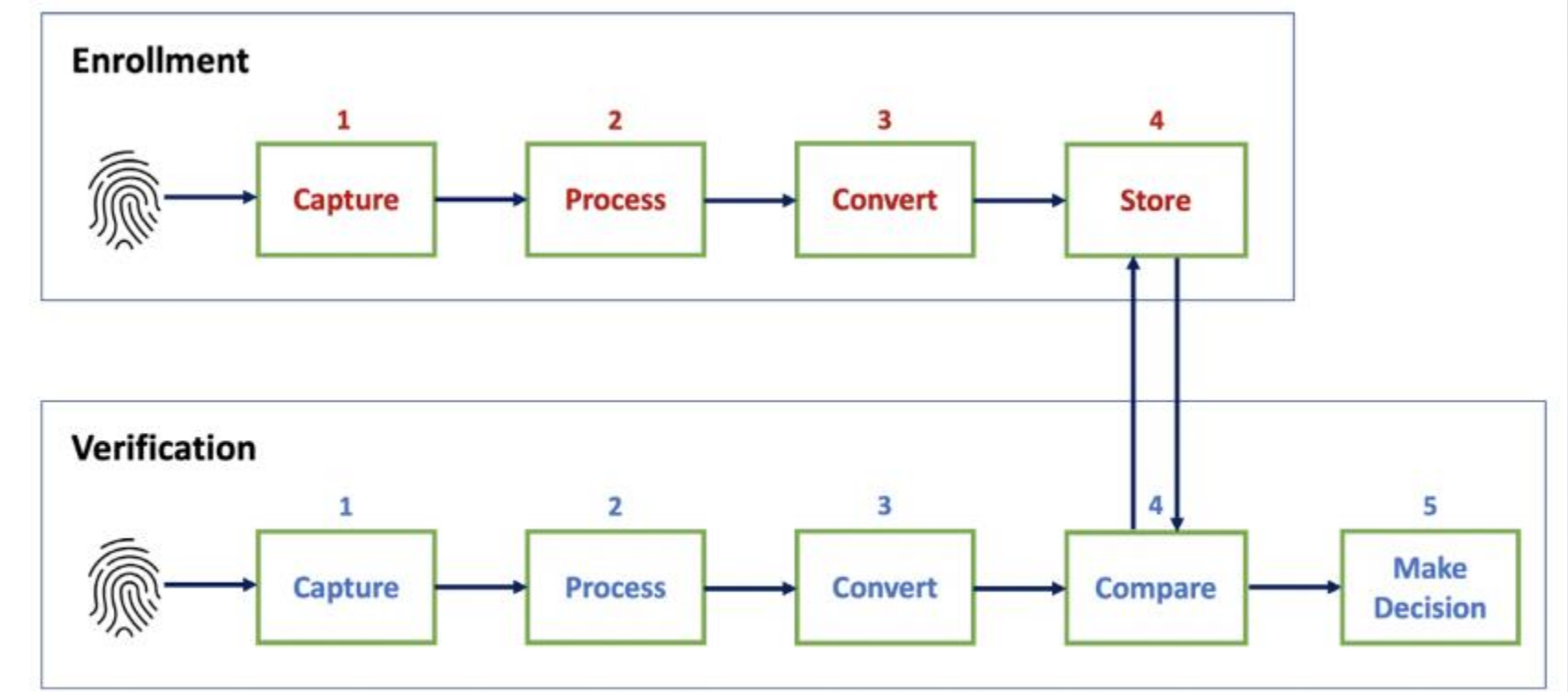


Figure 2: Simplified Biometric Matching Model

https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8334-draft.pdf

Analyze fingerprints-based authentication

Ref: https://www.ncsc.gov.uk/collection/biometrics

1. What can be the attacks?
2. What are your suggestions to mitigate some of the mentioned attacks?

Fingerprints-based authentication security

Threat and counter measure examples

1. Presentation attack: Fake artefacts (false fingerprint) like using a plaster cast of a finger.

Counter measure: liveliness detection like detecting conductivity properties of human skin; oxygen levels of the blood in the finger; pulse measurements

2. Replay attack: A stored signal is replayed into the system ignoring the sensor, like replaying an old copy of a fingerprint image (bypassing the sensor or step 1 in verification).

Counter measure: authenticate the sensor using challenge/ response approach

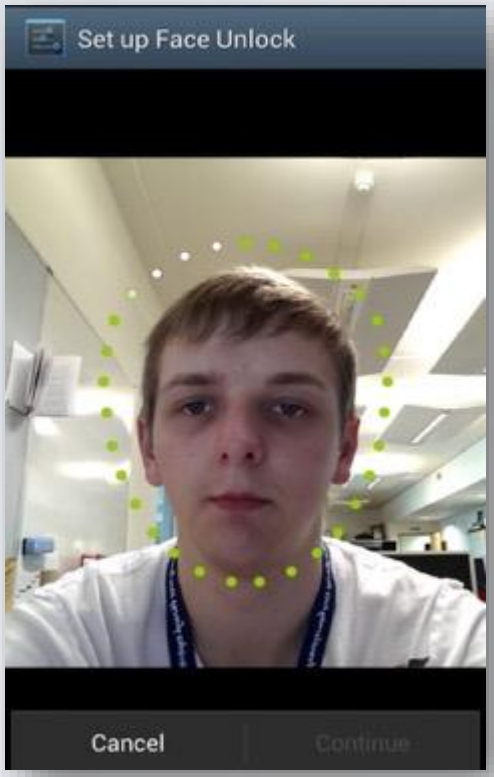
Fingerprints-based authentication security

3. Spoofing template (step 4 in Enrollment): fake one or more biometric templates in the database. As a result, either a fake identity is authorized or a rightful user face a denial of service.

Counter measure: protect the database with strong authentication/ authorization

The rationale for biometrics

Usability over Security?



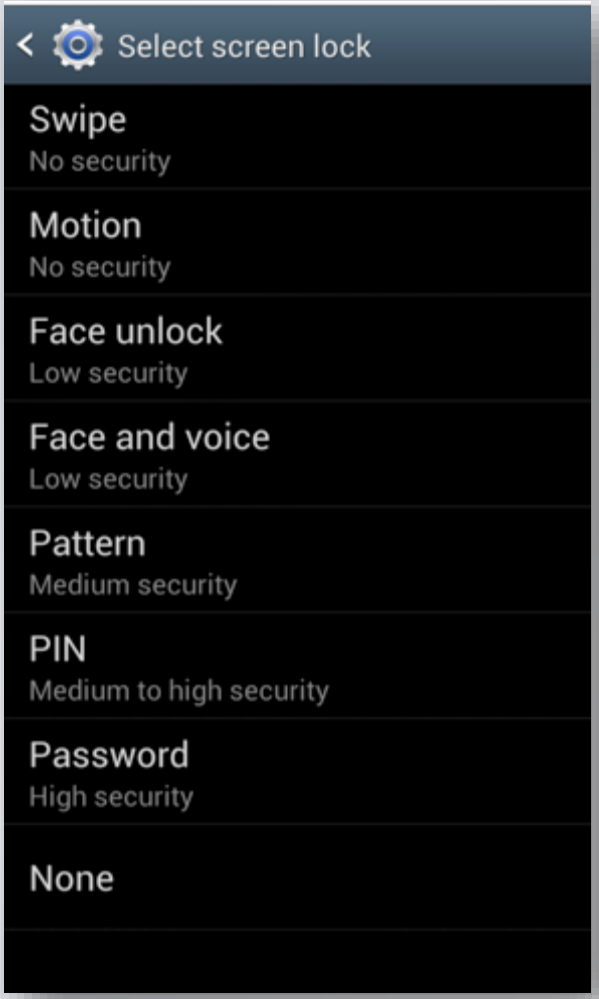
"*making each person's device even more personal*"

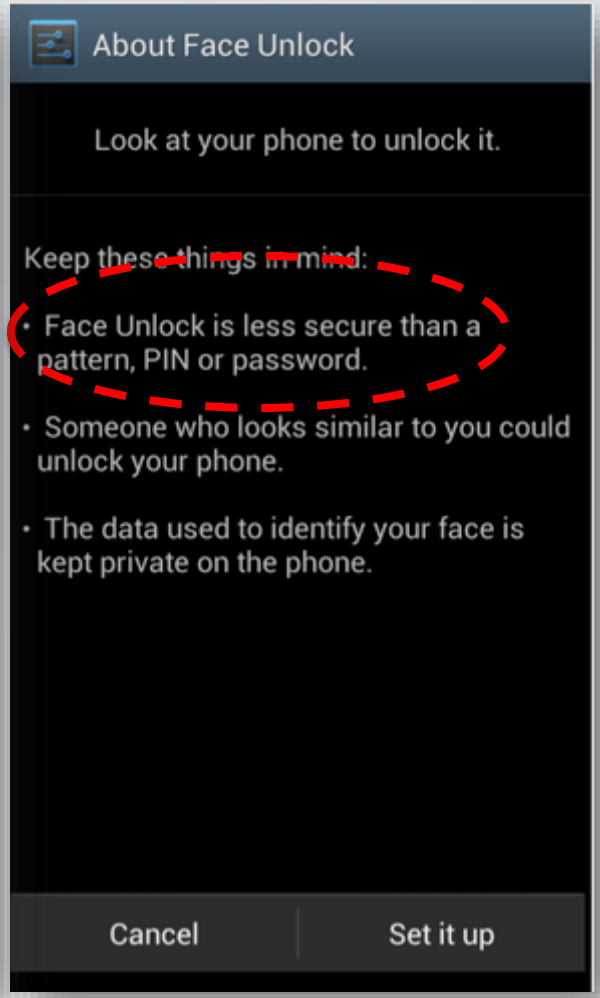
The advertising of Android Face Unlock (2011)

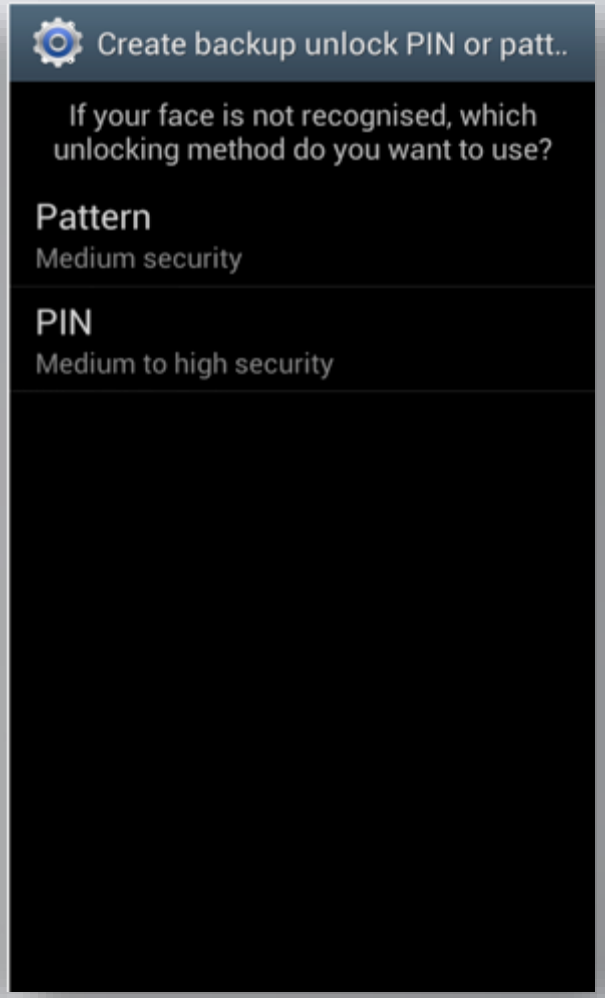
"*You check your iPhone dozens and dozens of times a day, probably more. Entering a passcode each time just slows you down*"

From Apple's promotional text for Touch ID (2013)

Ranking the protection







Analyze face recognition authentication

Ref (but not limited to):
https://www.ncsc.gov.uk/collection/biometrics

Rattani, A., & Derakhshani, R. (2018). A survey of mobile face biometrics

a) What are the cons? (classify them into security, mental effort,…)
b) What are the pros? (classify them into security, mental effort,…)
c) What can be the attacks and the counter measures? (classify them into the point of attacks/ attack surfaces)

Facial Flaws?

- Not a universal solution
  - reverts to PIN/password entry in low light conditions
- Questionable security
  - original version could be fooled by static photo of the legitimate user
  - limited Liveness detection (blink checking) introduced in mid-2012, but can still be fooled by edited photo

Needs more than just a liveness check

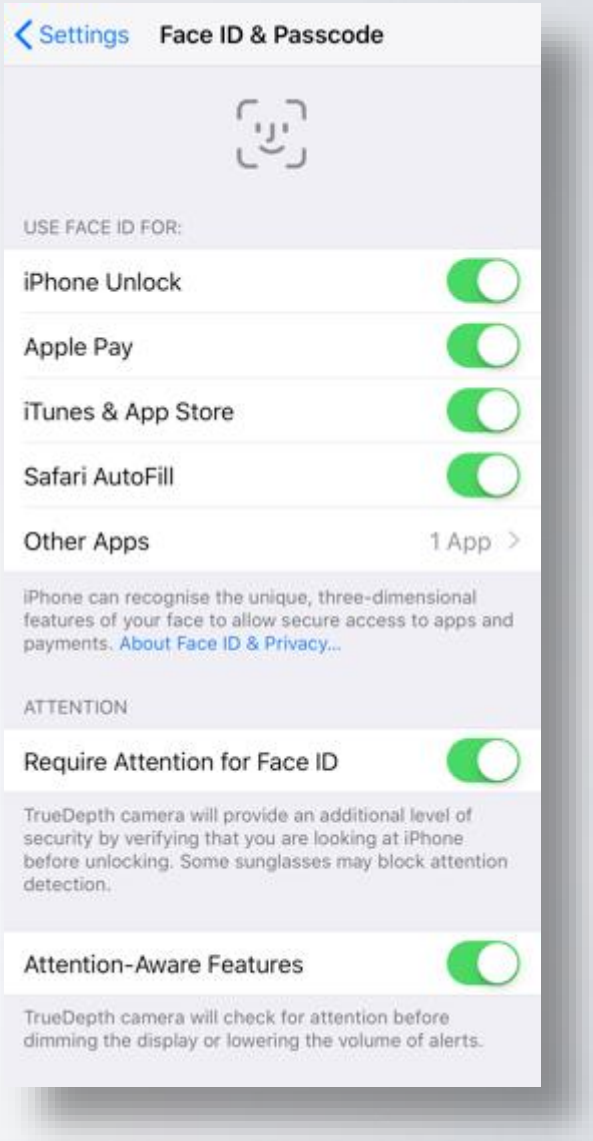
The unidentified Iranian woman reportedly used her husband's fingerprint to unlock his phone while he was asleep, before becoming incensed by what she found on the device.

-- used her mother's thumb to unlock a phone and open the Amazon app as mom napped on the couch just days before Christmas, The Wall Street Journal reported.

Little Ashlynd ordered 13 Pokemon gifts for herself, and told her parents she was "shopping" when they thought their Amazon account was hacked. The 6-year-old at least reassured her parents though that she got the shipping address right.

More robust methods

- Liveness detection and attention awareness
  - so things cannot be used when you are dead or asleep
- More than just PoE (point of entry)authentication
  - Payments
  - AutoFill
  - In-app authentication



So, farewell to passwords?

HSBC Bank flyer (Oct. 2016)

Bypassing Biometrics

Improve authentication

- Improve security with
  - multi factor authentication
  - multi step authentication
  - multi-biometrics authentication
  - continuous/ periodic authentication
- Improve usability with
  - transparent authentication
  - differentiated authentication
  - single-sign-on (SSO)
    [https://www.onelogin.com/learn/how-single-sign-on-works]

Single sign on

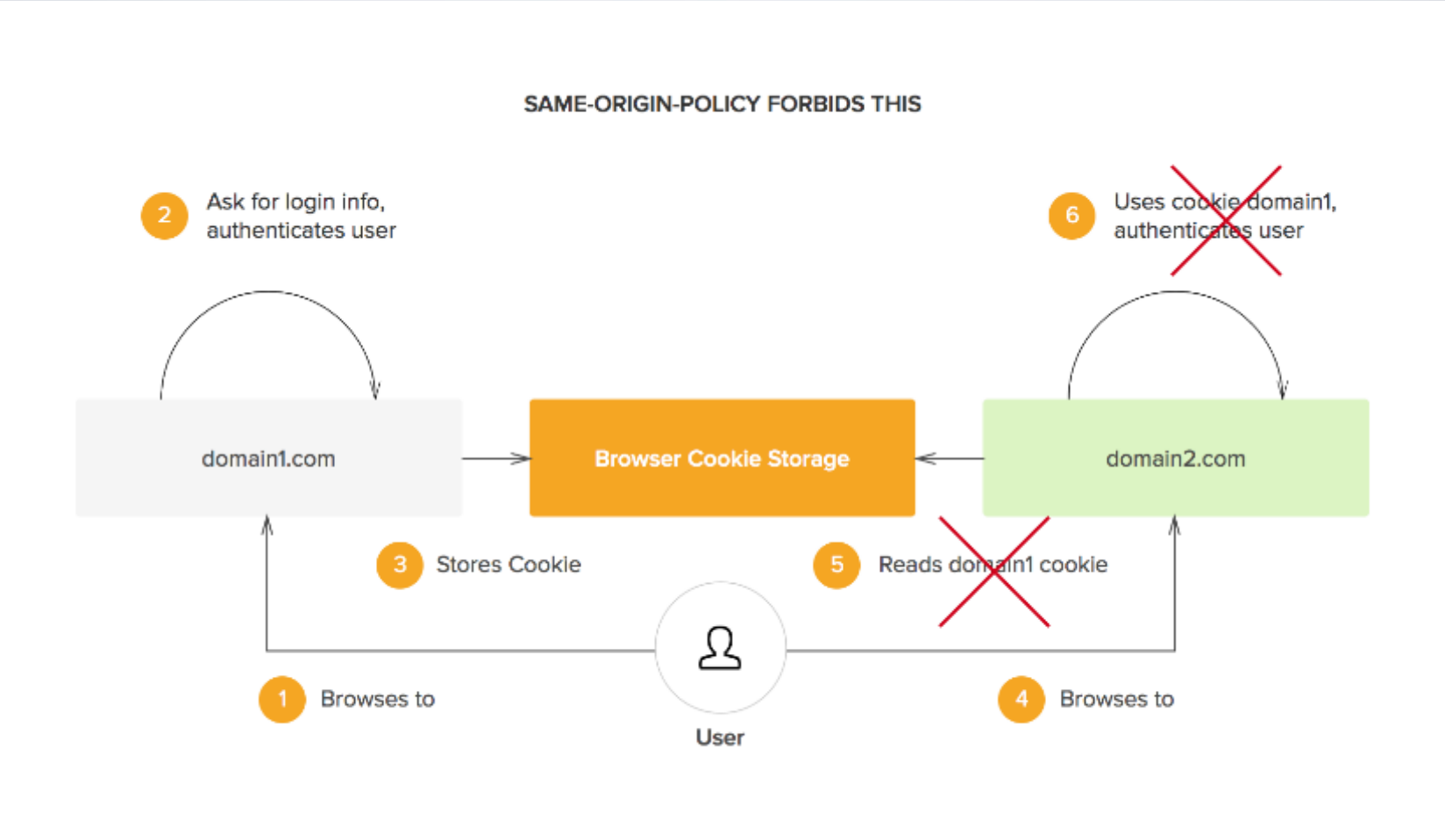
- An authentication method that enables users to log in with a single ID to any of several related, yet independent, software systems.
- Works based upon trust between an application (known as the service provider) and an identity provider

Session, cookies, token

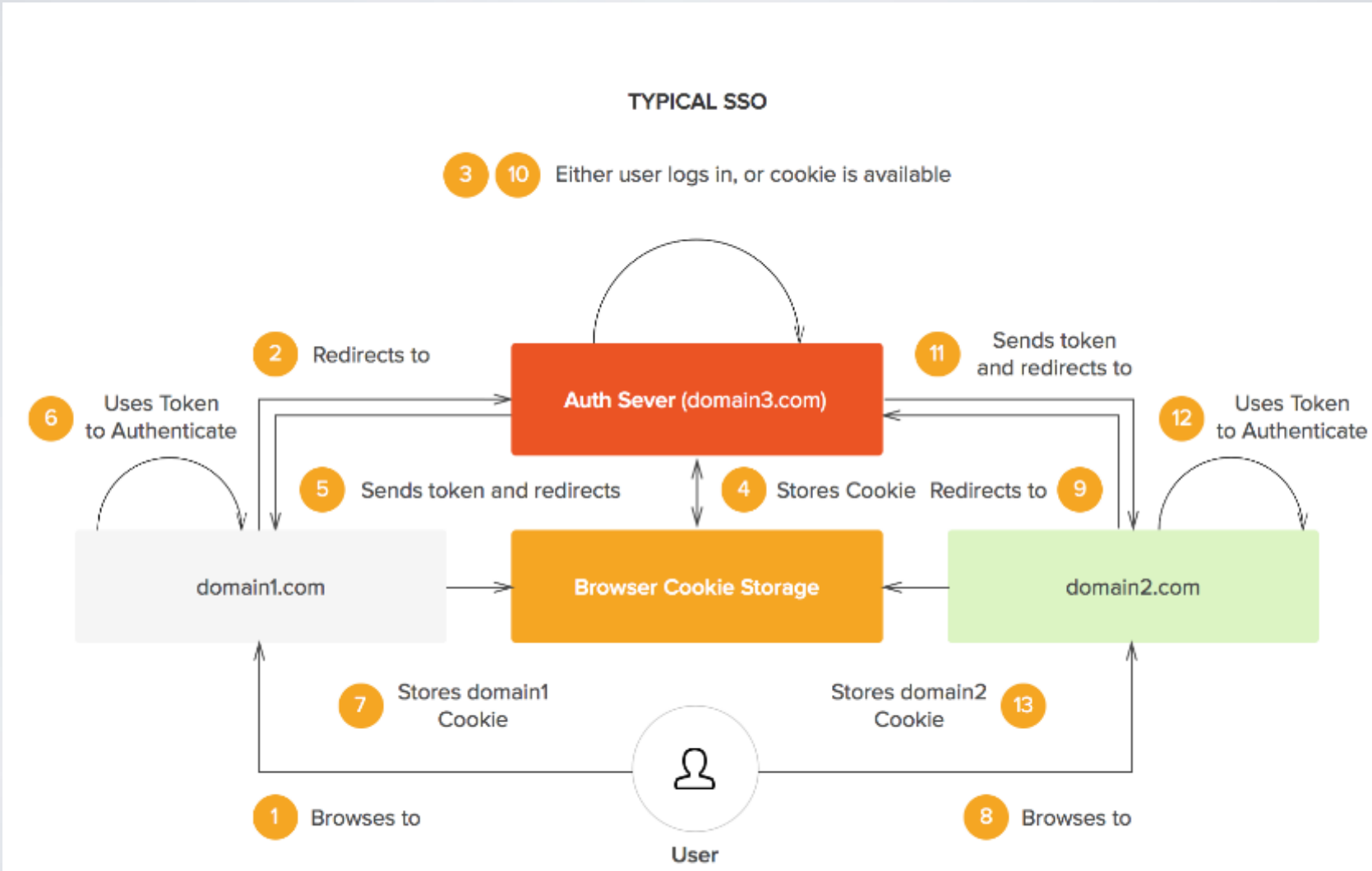
- HTTP sessions allows Web servers to maintain user identity and to store user-specific data during multiple request/response interactions between a client application and a Web application
- HTTP cookies: small blocks of data created by a web server while a user is browsing a website and placed on the user's computer or other device by the user’s web browser
- An authentication token (security token) is a hardware or software device required for a user to access an application or a network system in a more secure way

Without Single Sign On

Share session information across different domains?

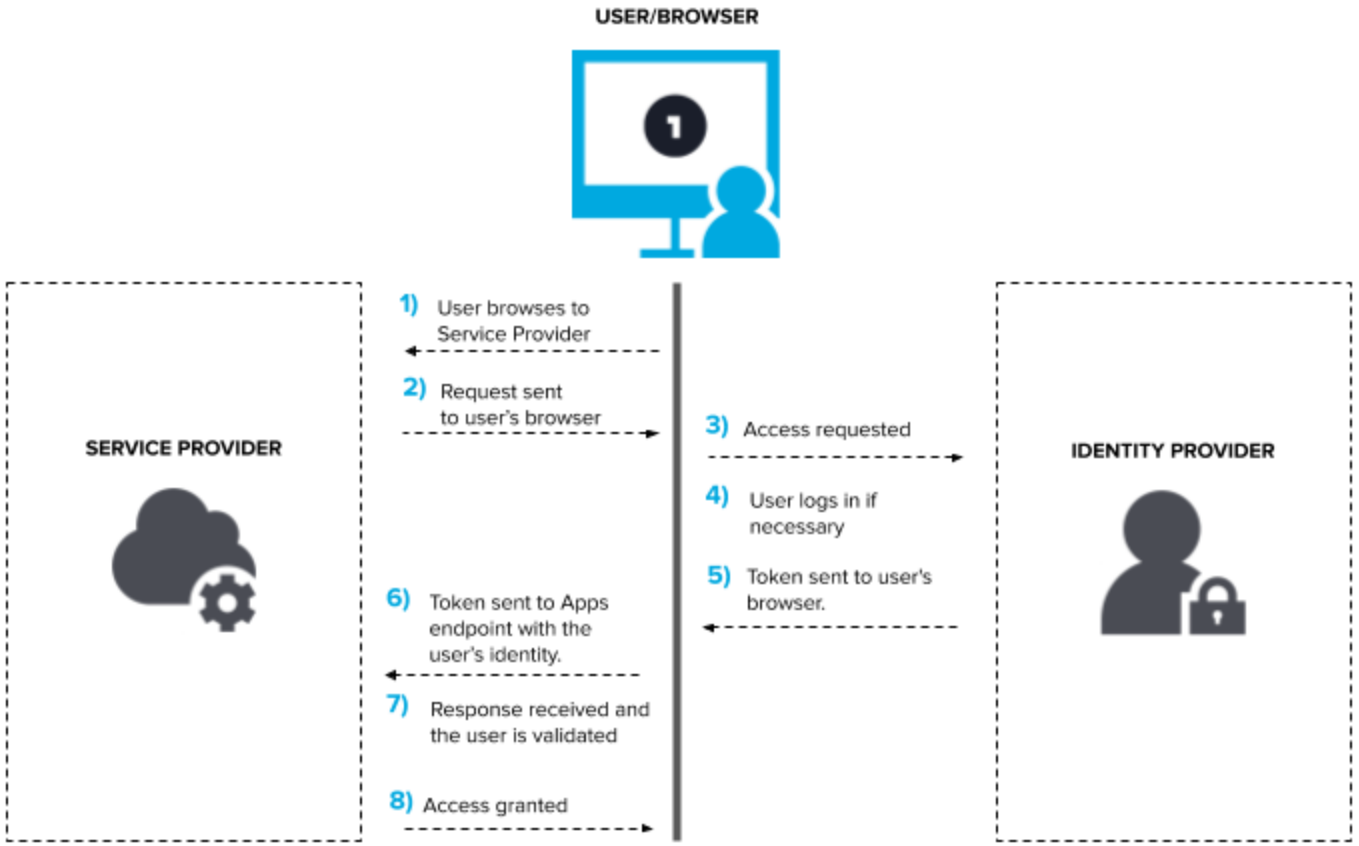


With Single Sign On



Entities in Single Sign On

Service Provider Initiated Workflow



Use case

- **Scenario:** A 10-person consulting firm sent a small team to South America to complete a client project. During their stay, an employee used a business debit card at a local ATM. A month after returning to the US, the firm received overdraft notices from their bank. They identified fraudulent withdrawals of $13,000, all originating from South America. There was an additional $1,000 overdraft fee.
- **Attack:** The criminals installed an ATM skimmer device to record card account credentials. Many false debit cards were manufactured and used at ATMs in different cities across South America.
- **Question**:
  - What are the used authentication factors? menti
  - What are your advice for the users, the company, and the banks to avoid such attacks in the future? menti

Future Authentication

One size fits all?

- Traditional authentication tends to deliver full access in one go
  - secondary authentication sometimes required for specific applications or services
- Potentially desirable to differentiate the requirement based upon the nature of the device/system, data, or level of access concerned but to manage it *transparently* wherever possible

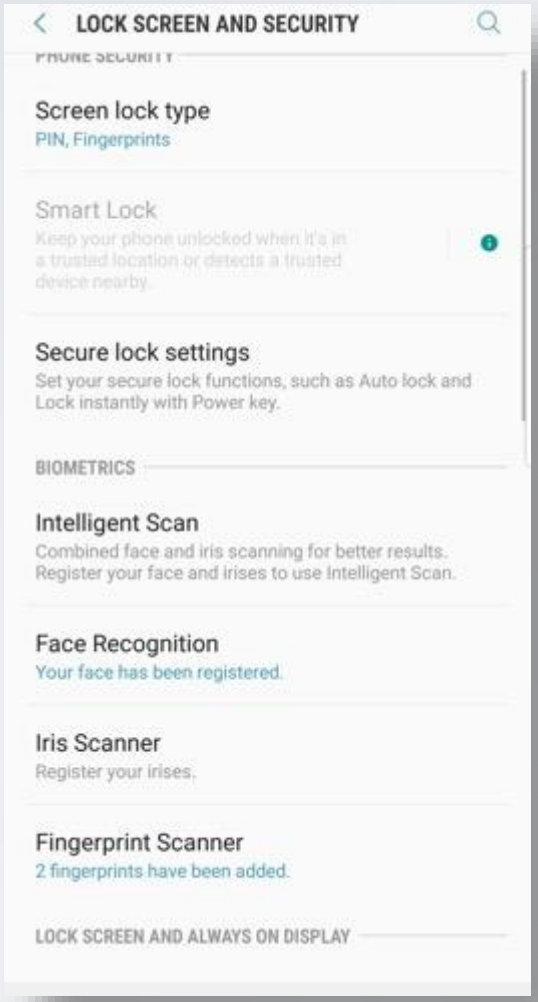
Transparent, Non-intrusive authentication

- Relevant to consider how to bring authentication strength and convenience together in a more effective manner
- Non-intrusive methods aim to maintain tolerability while offering opportunity beyond Point of Entry
  - ability to obtain a continuous (or periodic) measure of authentication
  - leveraging natural user interactions as a basis for collecting authentication data

Requirements

- Reduce the authentication burden upon the user
- Improve the level of security being provided
- More closely link authentication of the user with the subsequent request for access
- Ensure that the approach is commensurate with the needs of the access request
- Provide a more effective measure of identity confidence that goes beyond a simple Boolean decision

Multi-biometrics today



Screenshots from Samsung S9

Authentication Aura

- Improving the experience for multi-device users
  - recent authentication on one personal device reduces the need for explicit authentication on other devices in close proximity
- Aura level affected by strength of authentication method and how recent
  - can be maintained by non-intrusive monitoring and boosted by further explicit authentication actions
  - dissipates over time without further authentications
- Devices (and data) accessible based upon their sensitivity and current Aura level

Authentication Aura

Medium value
asset
(Partial access)

High value
asset
(Aura not strong enough,
No access)

Low value
asset
(Full access)

The strength of his Aura permits access to some devices but not others

Current Practice

A login password has been set for this user Change Password...

Require password immediately after sleep or screen saver begins

Show a message when the screen is locked Set Lock Message...

Allow your Apple Watch to unlock your Mac

What is authorization?

- menti

Authorization/ Control access

- An identity permits access to resources
- Authorization limits a *subject*'s access perform an *operation* on an *object*
  - Subject: for whom an action is performed
  - Object/ resource: upon what an action is performed
  - Operation: the type of action performed
  - Permission: the combination of object (resource) and operations allowed
  - Resource owner: who owns the resource

Example

- Identify the, object/ resource, operation, permission in the example:

“Alice shares the report in Onedrive with Bob but only allows him to read. Bob cannot edit the file”

Resource owner: Alice

Subject: Bob

Resource: the report in Onedrive

Operation: read, edit

Permission: Bob can read, Bot cannot edit

Role-based Access Control (RBAC)

- Users are assigned roles and are authorised to execute the operations linked to their active role.

Attribute-based Access Control (RBAC)

- *“logical access control methodology where authorisation to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes”*.

Example

Menti

Identify the type of access control and the resource, resource owner, role or attribute, operation, permission and its condition

Example 1: An online store sells alcoholic beverages. A user of the online store needs to register and provide proof of their age to be able to buy the alcohol.

Example 2: The University's DLE system allows students to view the content of COMP1002 class, but does not allow editing. They allows lecturers to view and edit the page.

Conclusions

Conclusions

- The range of authentication options has grown
  - still no single solution that us universally applicable and effective
- Predictions:
  - passwords will be with us for some time yet
  - other approaches (particularly biometrics) will become more commonplace

Looking ahead
More holistic protection?

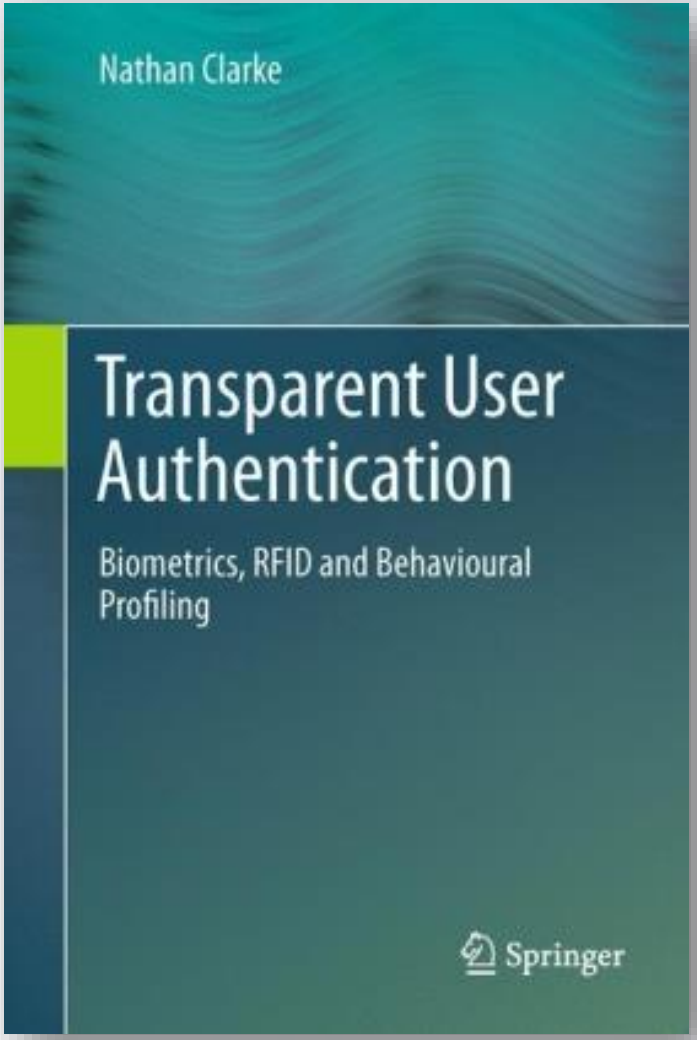
- Today's authentication is still largely PoE, with occasional re-verification for specific tasks
- Biometrics can contribute towards frictionless authentication
  - implemented transparently in parallel with normal use

2-min paper

- Menti, individual

1. Write down something you learn today that you did not know before
2. Write down something you are not still sure/ struggle with

Additional material



Additional material

“Biometrics: making the mainstream”

S.Furnell and N.Clarke.

Biometric Technology Today

January 2014, pp5-9

“Co-operative user identity verification using an Authentication Aura”

C.Hocking, S.Furnell, N.Clarke and P.Reynolds

Computers & Security

Vol. 39 (2013), pp486-502

SECURITY PODCASTS

FREE ON ITUNES U

LECTURES, DISCUSSIONS, INTERVIEWS, TUTORIALS, INDUSTRY INSIGHTS ...

www.cscan.org/podcasts

UNIVERSITY OF PLYMOUTH

Dr Hai-Van Dang
hai-van.dang@plymouth.ac.uk

Centre for Security, Communications & Network Research
www.plymouth.ac.uk/cscan