



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

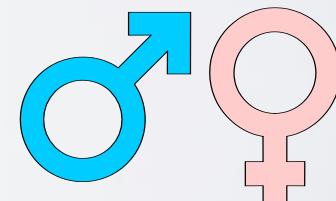
- Often not authenticating for a true security purpose

- 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!

ZDNet
MUST READ: ARE 8 NEW 'SPECTRE-CLASS' FLAWS ABOUT TO BE EXPOSED? INTEL CONFIRMS IT'S READYING FIXES

Windows 10: We're going to kill off passwords and here's how, says Microsoft

Microsoft wants to banish 'inconvenient, insecure, and expensive' passwords. So what's going to replace them?

By Steve Ranger | May 2, 2018 -- 13:14 GMT (14:14 BST) | Topic: Enterprise Software

CNET

Google security exec: 'Passwords are dead'

Special show: Google's security exec says 'passwords are dead'.

betanews

Hot Topics: Windows 10 | Microsoft | Apple | Cloud | Tablets | Android | Security | Reviews

Passwords are dead

By Ray Walsh | Published 6 months ago

18 Comments G+1 Tweet

recode

MEDIA SECURITY VOICES

Passwords Are Dead. Long Live Multifactor Authentication.

President Obama's appeal to "move beyond passwords" is critical to a secure digital future.

BY CHRIS WEBBER | MAR 16, 2016, 6:00AM EDT



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

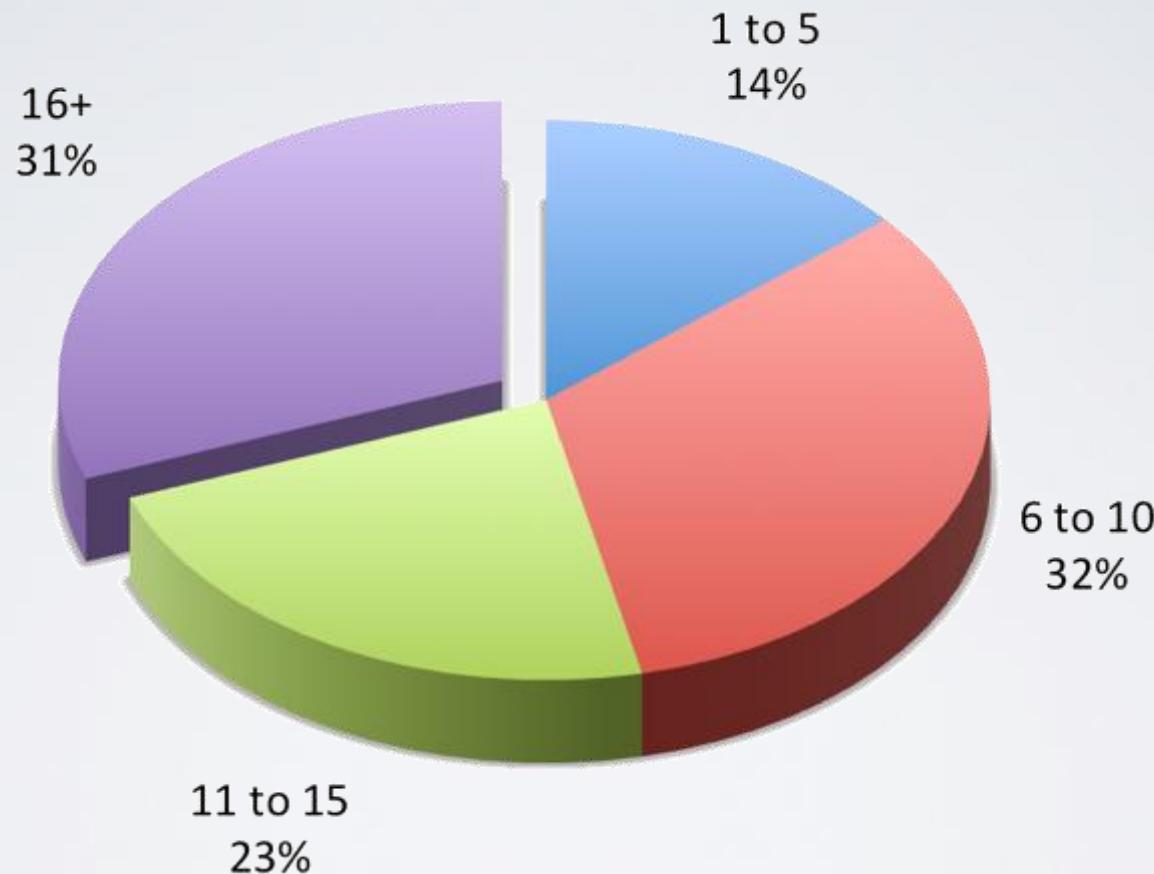
- Easy to get the idea
- Familiar from other systems
- Can be made to work in most contexts (devices/systems/sites)



● Cons

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

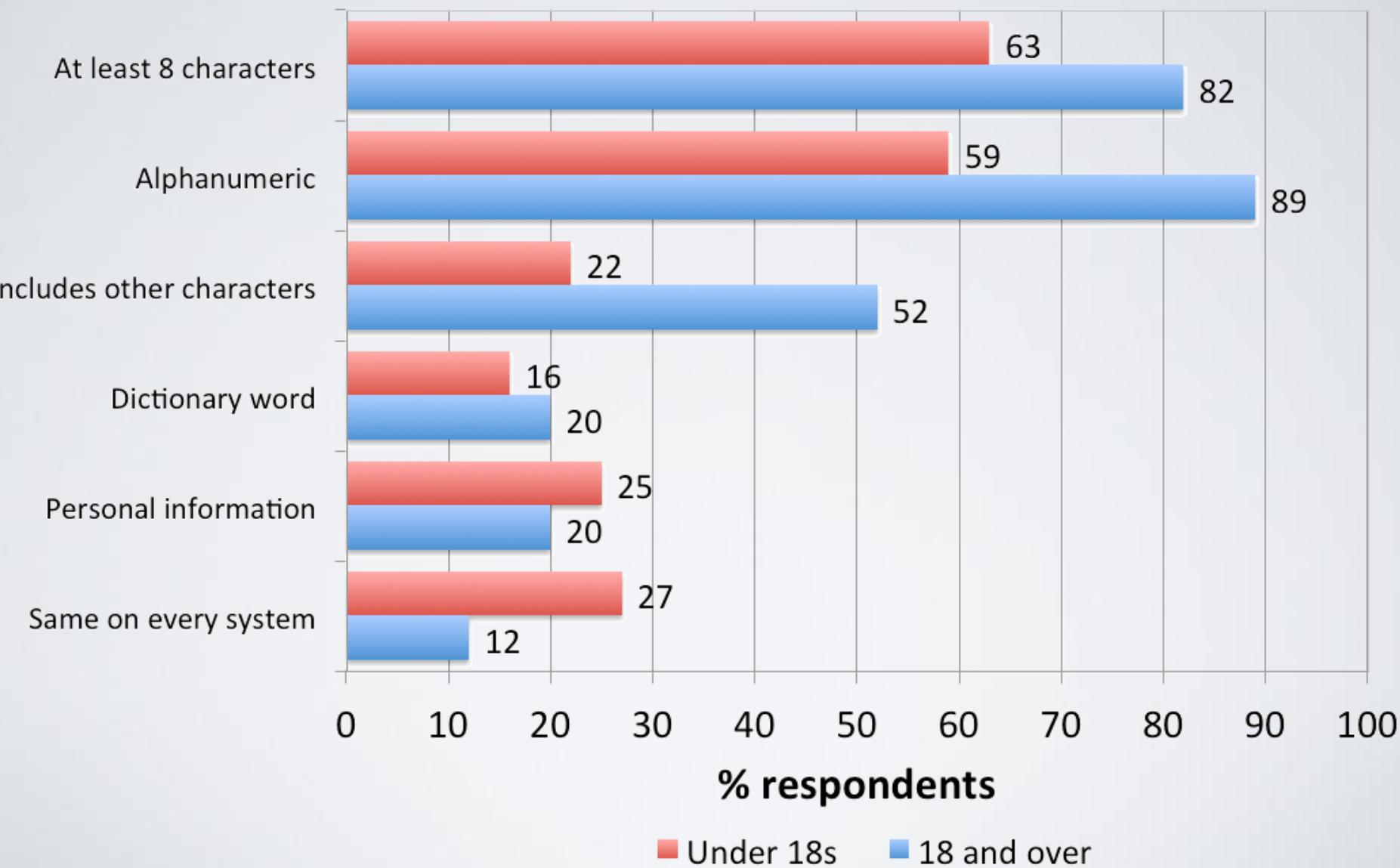
Lots to remember? How many passwords?



(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 passwordsAnalysis 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

pscrack LC5 - [Untitled1]

File View Session Schedule Remediate Help

Run Report

Domain	User Name	LM Password	c8	Password	LM Hash	NTLM Hash
[REDACTED]	ASPNET				291C98386F829019C4912B765295988D	F73650
[REDACTED]	BackupSysAdmin				AF89AECEC8DCB14FF26806ECC96527F2	F32EAA
[REDACTED]	Guest	* empty *	x	* empty *	AAD3B435B51404EEAAD3B435B51404EE	31D60FF
[REDACTED]	LUKE23		x	luke23	004041B8E7E5D97CAAD3B435B51404EE	55315AA
[REDACTED]	SQLDebugger	* empty *			AAD3B435B51404EEAAD3B435B51404EE	F573A6D
[REDACTED]	Administrator	???????			1F78295A8FA5B987B79AE2610DD09D4C	4B543FD4

DICTIONARY/HYBRID

words total	29156
words done	0
% done	0.000%

HYBRID

hash tables	0 of 0
hashes found	0 of 0
% done	0.00%

BRUTE FORCE

time elapsed	0d 0h 0m 0s
time left	
% done	

current test

keyrate

SUMMARY

total_users	6
audited_users	2
% done	33.333%

NM

The screenshot shows the pscrack tool interface. On the left is a table of user accounts with their domain, user name, LM password, c8 password, LM hash, and NTLM hash. The 'Guest' account is highlighted with an orange background. On the right is a status panel with sections for 'DICTIONARY/HYBRID', 'HYBRID', 'BRUTE FORCE', and 'SUMMARY'. A red circle highlights the 'DICTIONARY/HYBRID' section, which displays statistics like 'words total' (29156), 'words done' (0), and '% done' (0.000%).

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?



Would you like to save this password?

To review or remove passwords you have saved, open [Safari preferences](#), and then click [Passwords](#).

[Never for this Website](#)

[Not Now](#)

[Yes](#)

And what about here?

New password



Use Safari suggested password:
NXJ-JfM-PeU-YQ8

This password will be saved in your iCloud Keychain
so it is available for AutoFill on all your devices.



show password

AutoFill in action

Provides it for me at Login ...

The screenshot shows the ECAS login interface. At the top, there's a header with the European Commission logo and the text "EUROPEAN COMMISSION AUTHENTICATION SERVICE (ECAS)" and "External". Below the header, a breadcrumb navigation shows "EUROPA > Authentication Service > Login". On the left side, there's a large ECAS logo with the text "authenticates your identity on European Commission websites". The main area contains a "Login" button, a "New password" link, a "Sign Up" link, and a "Help" link. A message asks if the selected domain is correct, with "External" and "Change it" options. Below this is a form for entering a "Username or e-mail address" (which is filled with a yellow placeholder) and a "Password" (which is also filled with a yellow placeholder). There's a "More options..." link, a "Login" button, and a "Lost your password?" link. A note indicates that fields marked with an asterisk are required. At the bottom, there's a section for alternative logins with icons for "Mobile phone", "Token", and "eId".

EUROPEAN COMMISSION AUTHENTICATION SERVICE
(ECAS)

External

EUROPA > Authentication Service > Login

Login New password Sign Up Help

Is the selected domain correct?
External Change it

Username or e-mail address *

Password *

More options...
Login Lost your password?

* Required fields

Or log in with your

Mobile phone Token eId

AutoFill in action

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

The screenshot shows the ECAS Signature page. At the top, there's a logo for the European Commission and the text "EUROPEAN COMMISSION AUTHENTICATION SERVICE (ECAS)". Below that, it says "External". The navigation bar includes links for "EUROPA", "Authentication Service", and "ECAS Signature". On the right side of the header, there are links for "Logout", "Change password", "Account information", and "Help". A user profile is shown with the name "Steven FURNELL" and "External".

ECAS Signature

Welcome Steven FURNELL to the ECAS Signature page. This page allows you to digitally sign a transaction using your ECAS password.

The Participants Portal application is asking you to sign a transaction. The transaction has the following description: **This is your legal commitment**.

[See the complete transaction](#) [Printer-friendly Version](#)

To sign the transaction, please enter your ECAS password.

Reason: **By entering your ECAS password, you can sign this legal commitment electronically.**

Password *

* Required fields

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>

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



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.



Key logging

Installing a keylogger to intercept passwords when they are entered.



Shoulder surfing

Observing someone typing in their password.



Phishing & coercion

Using social engineering techniques to trick people into revealing passwords.



Brute force

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



Manual guessing

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



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.



Password spraying

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



Data breaches

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



...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.

Protect all passwords



1. Ensure corporate web apps requiring authentication use HTTPS.
2. Protect any access management systems you manage.
3. Choose 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.

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.

Implement technical solutions



1. Throttling or account lockout can defend against brute force attacks.
2. For lockdown, 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.

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.

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.

Multi-factor authentication



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

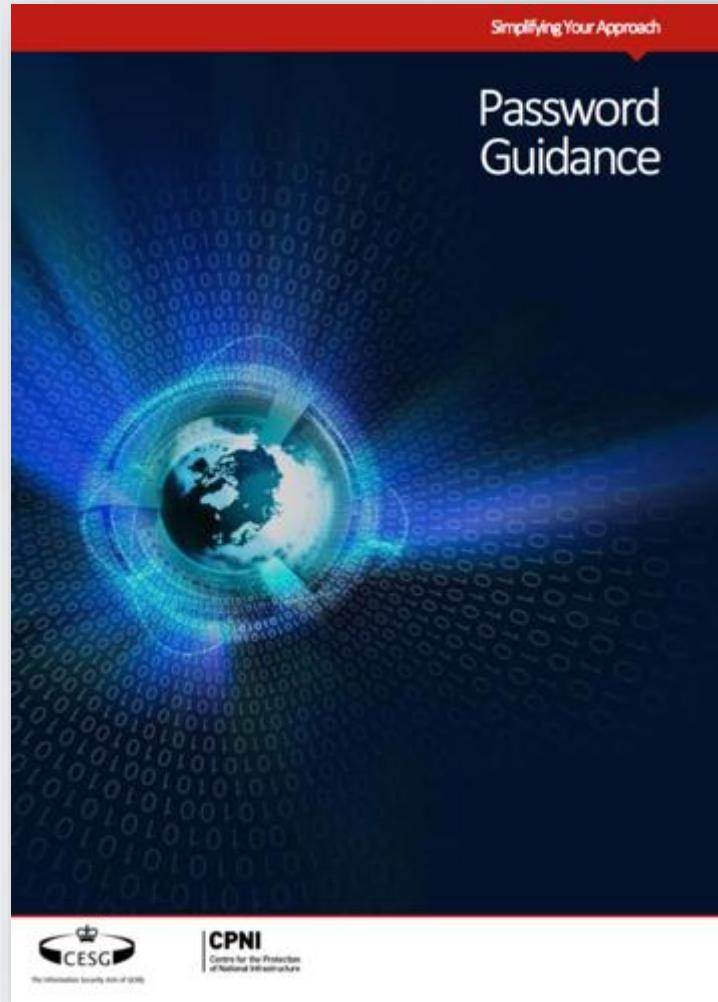
Improving Password Systems

- 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 advises *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 . . .

RATE YOUR PASSWORD WITH PLYMOUTH UNIVERSITY

Try to create a strong password:

.....

Show Password

a A 1 !

Comments:

Your password contains 16 or more characters and should be safe from a brute force attack.

It would take a fast computer approximately 109939505232854990 years to guess your password.

Tips for strong passwords:

- ✓ Use at least 8 characters
- ✓ Use both upper and lower case letters
- ✓ Use more than one number
- ✓ Use symbols (!,@,#,\$,%,&,*?,_,~)

For help on protecting yourself online, download our [free guide](#).

	Strength
Score:	100%
Rating:	Very Strong

Scoring Information:

18 points (36%) for length (16)
1 point (2%) for at least one lower case char
5 points (10%) for at least one upper case char
5 points (10%) for at least one number
5 points (10%) for at least three numbers
5 points (10%) for at least one special char
5 points (10%) for at least two special chars
2 combo points (4%) for upper and lower letters
2 combo points (4%) for letters and numbers
2 combo points (4%) for letters, numbers and special chars

www.cscan.org/passwordstrength/

And another one . . .

The screenshot shows the Kaspersky Secure Password Check interface. At the top, there's a language selection bar with 'English' and a dropdown arrow. Below it is the Kaspersky logo with the text 'SECURE PASSWORD CHECK'. A yellow warning box contains the text 'Never enter your real password' with an exclamation mark icon, followed by a smaller note: 'This service exists for educational purposes only - Kaspersky Lab is not storing or collecting your passwords.' To the right of the warning box is a close button 'X'. Below the warning box is a password input field containing '.....' with a red asterisk (*) to its right. Underneath the input field is a progress bar consisting of four colored segments: red, orange, yellow, and green. Below the progress bar, a message states: 'Your password will be bruteforced with an average home computer in approximately'. A large red box displays the number '33' followed by 'YEARS' in white. To the left of this box is a white circle with black dots. To the right of the '33 YEARS' box is a green bar containing the text 'You can spend this time walking to the moon and back 1 time'. At the bottom, there are social media sharing icons for Facebook, Twitter, Google+, and LinkedIn.

Never enter your real password
This service exists for educational purposes only - Kaspersky Lab is not storing or collecting your passwords.

..... *

Your password will be bruteforced with an average home computer in approximately

33 YEARS

You can spend this time walking to the moon and back 1 time

f t g+ in

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

ebay

PICK YOUR SECRET QUESTIONS

Give yourself another way to recover your account securely in case your information becomes outdated.

Question 1:

Name of favourite book?

Cybercrime: Vandalizing the Information Society

Answers are not case-sensitive, must not include symbols and should not be an answer that would frequently change.
Looks like you're using a symbol we don't allow.

Question 2:

Select an option

Answer

Question 3:

Select an option

Answer

Confirm

Cancel

First company you worked for?

Name of favourite book?

Model of your first car?

Name of your first pet?

Last name of favourite actor?

Name of your favourite band or singer?

Dream job as a child?

City where you met your other half?

City/country where you want to retire?

First name of your best friend?

Name of the street you grew up on?

Name of favourite film or series?

Your childhood nickname?

First name of your oldest cousin?

First name of best man or maid of honour?

First three words of favourite quote?

First name of your favourite boss?

Choose your own phrase (at least 2 words)

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 rather than precise 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



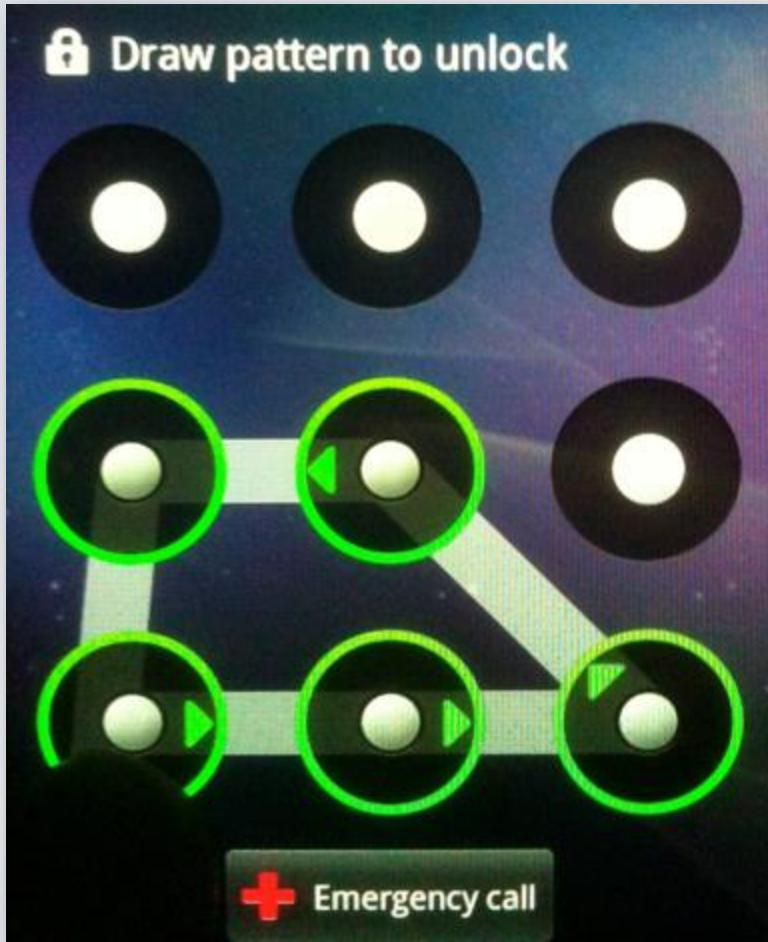
GOTPass (2015)

- 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

Please use the onscreen key pad below to enter your PIN and memorable date details

Please enter the 1st, 6th and 3rd digits of your PIN

<input type="text"/>	<input type="text"/>	<input type="text"/>
1ST	6TH	3RD

Please enter your memorable date in dd/mm/yy format

<input type="text"/>	<input type="text"/>	<input type="text"/>
DD	MM	YY

ING Direct Security

Remember: We will always ask you to use the keypad tool for partial entry of your pin. We will never ask you to provide your full pin when you login.

If you have any concerns about the information that you are asked to provide do not continue with your login, and contact us immediately on 0845 603 8888 or e-mail us at security@ingdirect.co.uk. To ensure you are protected from any internet threats please ensure your Antivirus, Antispyware and Firewall software is active and up to date.

At ING Direct we take the security of your account very seriously. Once you are an ING Direct customer we will never send you e-mails or call you asking for your login details (PIN or memorable date). If you receive any such request, please call us immediately on 0845 603 8888. From time to time, we may include embedded links in marketing e-mails you receive from us, which will make further information more accessible for you. To ensure you're fully aware about banking online securely, please visit [our security zone](#).

[If you are having trouble using the Key Pad please click here.](#)

To increase your online security please mouse click on the digits below to enter them into the highlighted PIN and memorable date fields.

9	4	6
2	7	8
5	3	1
0		

[Complete login ▶](#)

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, individual

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

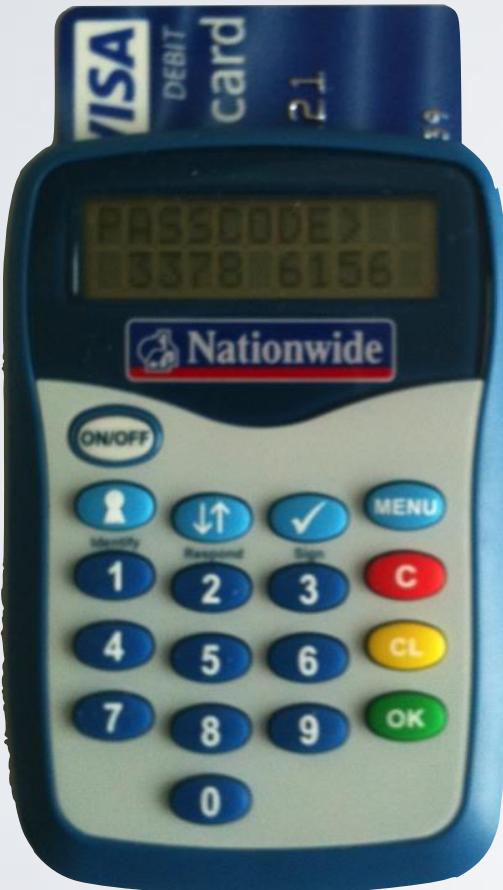
● Disadvantages

- 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

We're upgrading the way you log on to Personal Internet Banking

We need to help you replace your current log on details as part of an upgrade to your Internet Banking security.

You only need to upgrade once and it will take just a few minutes. So why not complete it now? To do this, you'll need your Secure Key which you should have received in the post.

Please select Continue, you can then either upgrade your Personal Internet Banking or skip to My Accounts.

[Not received your Secure Key?](#)



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)

Log on to Online Banking

You are logging on as: [REDACTED]

[Switch user >](#)

1. Select log on method

[With Secure Key](#)

[Without Secure Key](#)

Use your Secure Key to log on to full Online Banking

2. Answer your memorable question

What is your eldest child's middle
name? :

[Forgot your memorable question answer?](#)

3. Enter the **2nd, 5th and last** characters of your password

Password

 ...

[Forgot your password?](#)

[Forgot both your memorable question answer and your password?](#)

[Back](#)

[Continue](#)

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?

A screenshot of a Twitter post from an iPhone. The post features a large black redaction box at the top left. To its right is a small button with a blue Twitter bird icon and a plus sign. The main text of the tweet is: "you Internet banking. "your password requires uppercase letter, a number, a hair from the head of Jesus, asparagus, a rainbow & Yoda" (with the first word redacted). Below the tweet, it says "1 day ago via Twitter for iPhone". At the bottom are four grey navigation icons: a left arrow, a retweet/reload symbol, a star, and a right arrow.

[REDACTED] you Internet banking. "your password requires uppercase letter, a number, a hair from the head of Jesus, asparagus, a rainbow & Yoda"

1 day ago via Twitter for iPhone

← ↲ ★ →

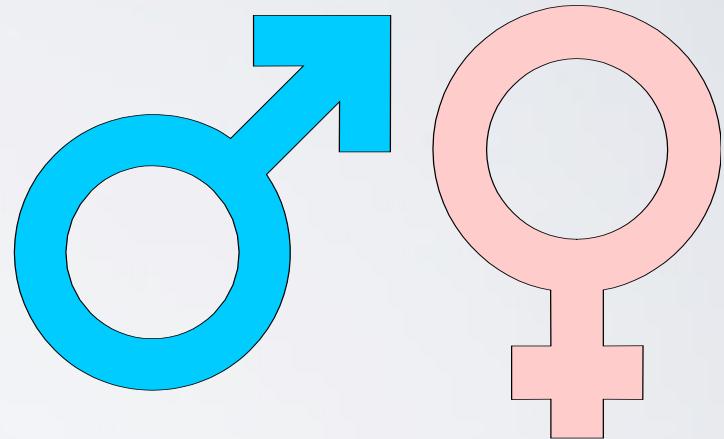
Biometrics

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*:

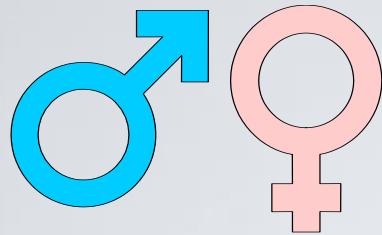
"A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition"

As a *process*:

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

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

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 Broxfield
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 Broxfield 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 Comstar Ltd.

Presented at SYSTEM SECURITY '87, Oxford Publishing, Oxford, UK, 1987

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

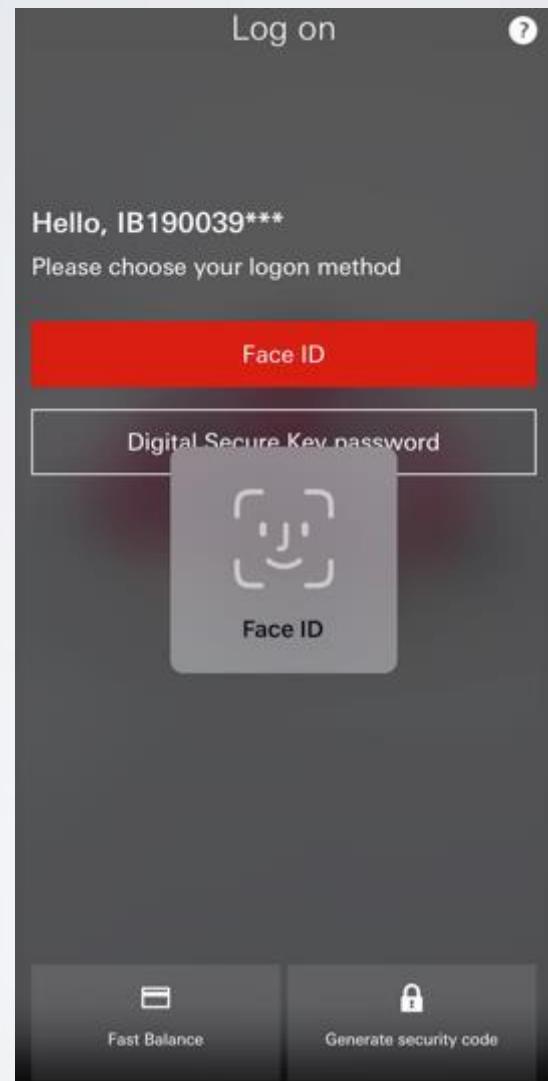
- Banks are backing biometrics
- Survey of 2,038 people, commissioned by HSBC
 - 55% rarely changed passwords
 - 74% felt that biometric security would become the default "password" of the future

BBC News

19 February 2016

<http://www.bbc.co.uk/news/business-35609833>

In the present . . .



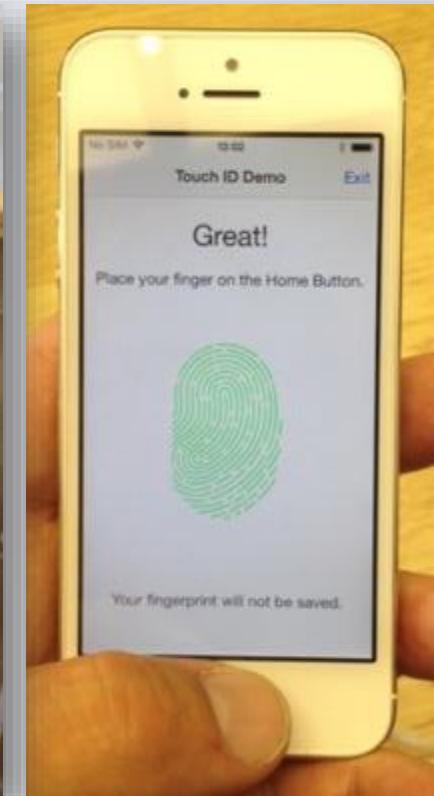
HSBC Mobile Banking app
February 2018

Biometrics in the past



HP iPAQ H5450 (2002)
and later models

Biometrics today



Lift and rest your finger on Touch ID repeatedly →

(
9

)
0

-
-

+
=

←

I

O

P

{
[

}
]

↔

:

"

|

5

The Rise of Biometrics

- Key rationale is ease of use

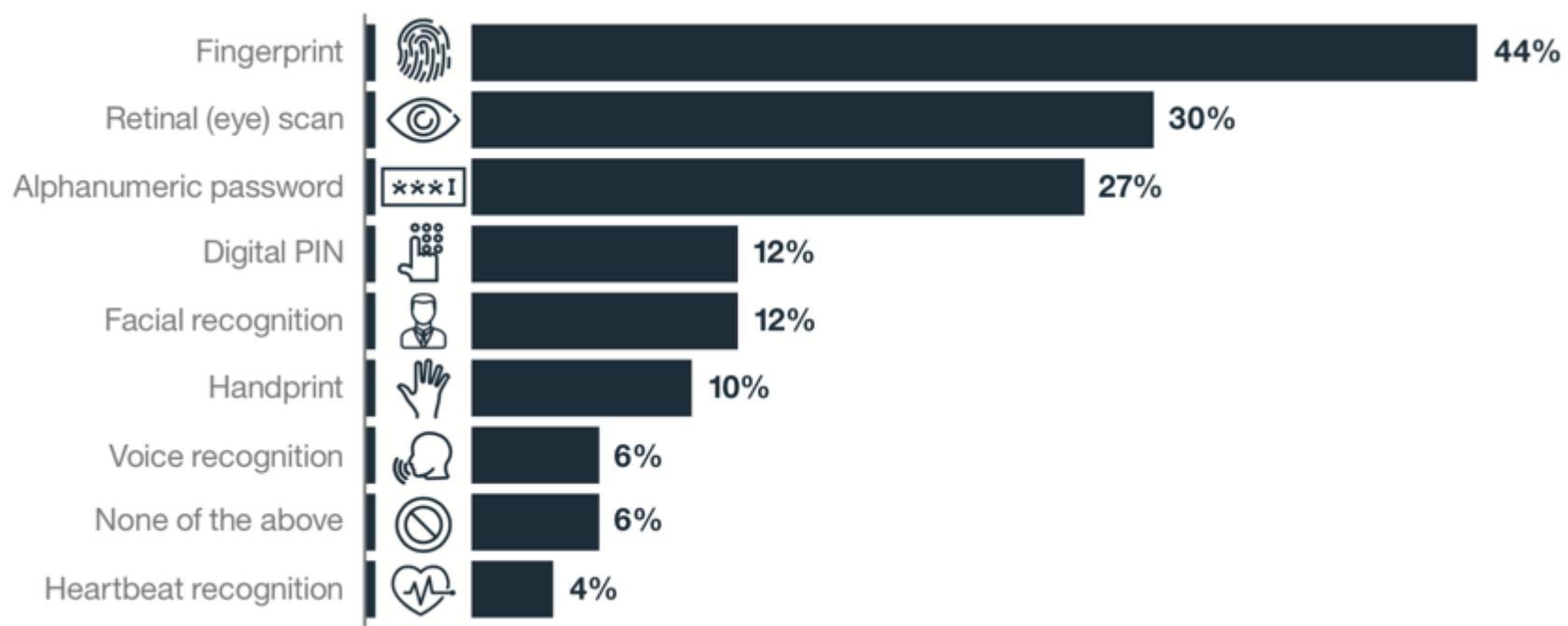
- a (correctly used) password can deliver security but becomes increasingly impractical
- we need usable alternatives

- 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)

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

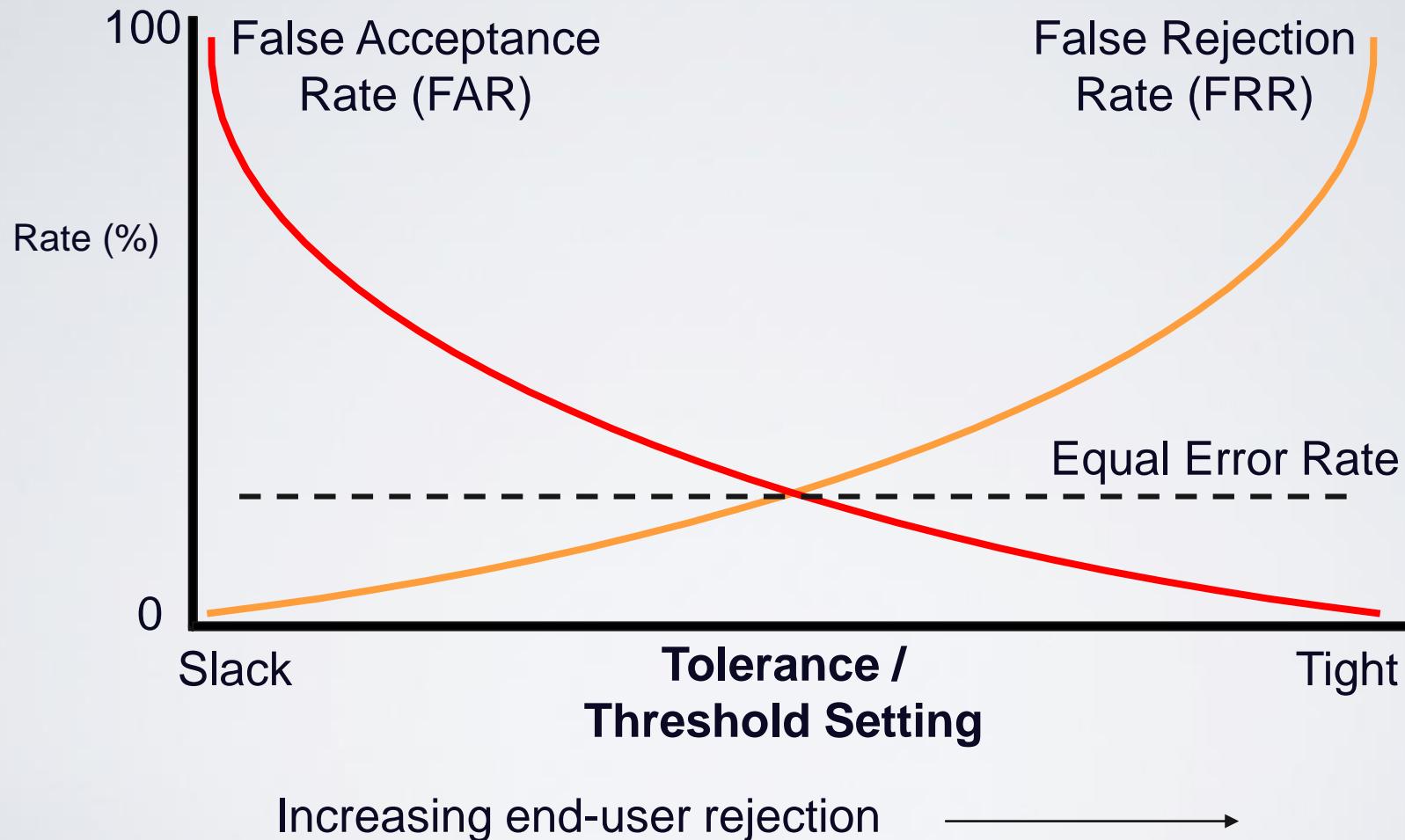
Compare biometrics-based system using FAR/ FRR

- 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%

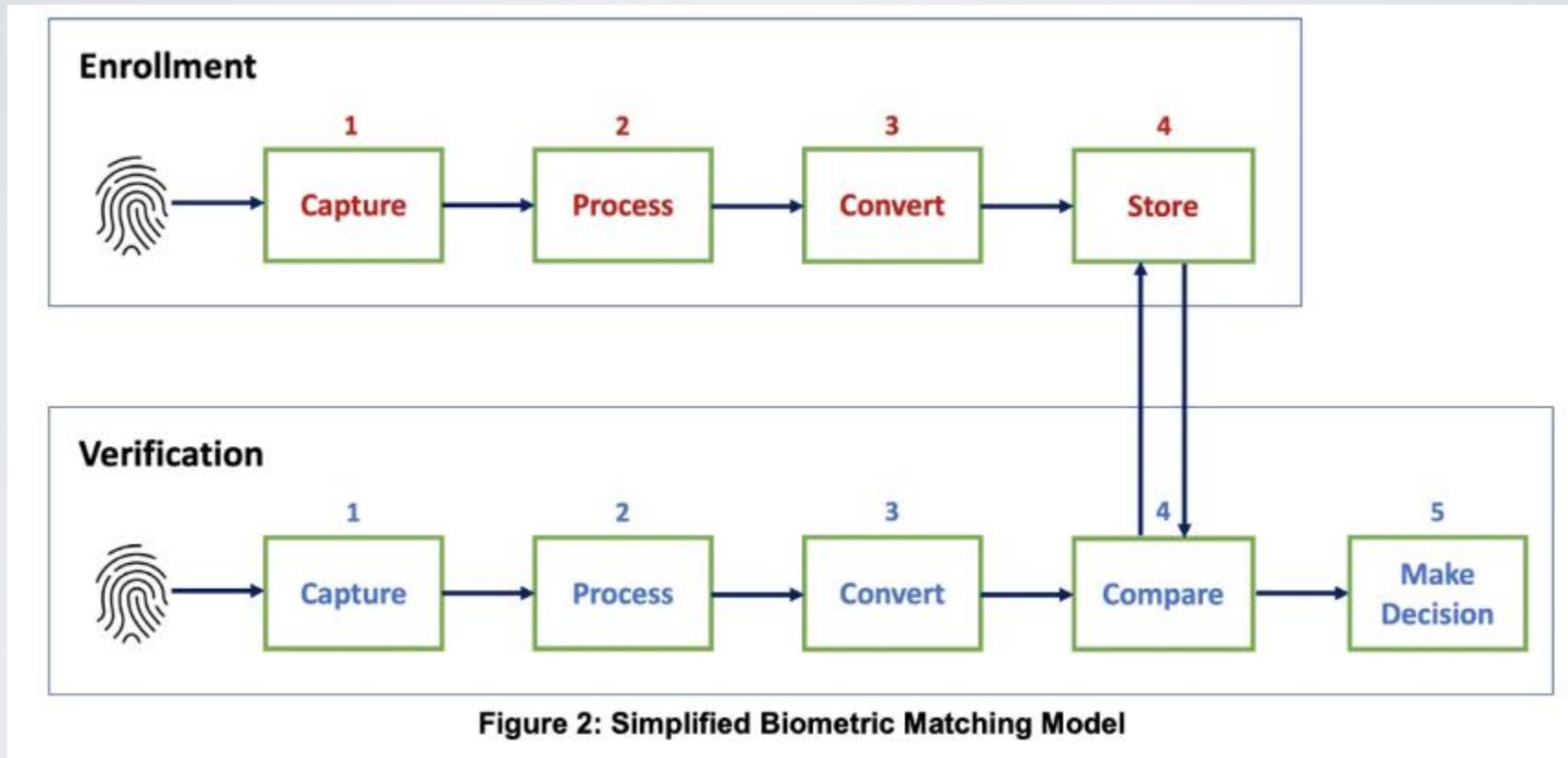
Which system is more secure?

Which system is more convenient?

FAR / FRR relationship



Simplified biometric matching model



<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

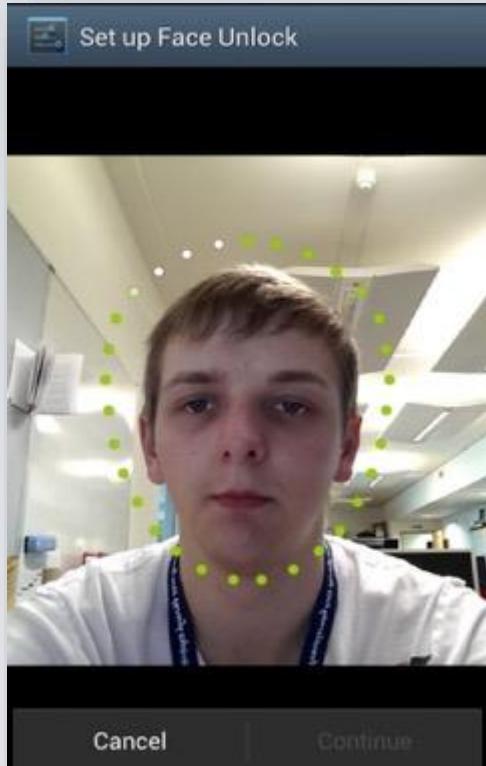
Fingerprints-based authentication security

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

< Select screen lock	
Swipe	No security
Motion	No security
Face unlock	Low security
Face and voice	Low security
Pattern	Medium security
PIN	Medium to high security
Password	High security
None	

About Face Unlock

Look at your phone to unlock it.

Keep these things in mind:

- Face Unlock is less secure than a pattern, PIN or password.
- Someone who looks similar to you could unlock your phone.
- The data used to identify your face is kept private on the phone.

Cancel Set it up

Create backup unlock PIN or patt..

If your face is not recognised, which unlocking method do you want to use?

Pattern
Medium security

PIN
Medium to high security

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?



- ➊ Not a universal solution
 - reverts to PIN/password entry in low light conditions
- ➋ 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 incident took place on a Qatar Airways flight / AFP/Getty Images

INDY/GO

FLIGHT DIVERTED AFTER WOMAN DISCOVERS HER HUSBAND IS CHEATING ON HER

The incident caused a mid-flight emergency

HELEN COFFEY
Tuesday 7 November 2017 17:31 GMT



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.



REVIEWS NEWS VIDEO HOW TO SMART HOME CARS

CULTURE

Child uses sleeping mom's fingerprints to buy Pokemon gifts

When you want to buy \$250 worth of Pokemon presents, desperate times call for desperate measures.

BY ALFRED NG / DECEMBER 27, 2016 6:25 AM PST

f t f o e m

-- 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

NON-SO SCENARIO

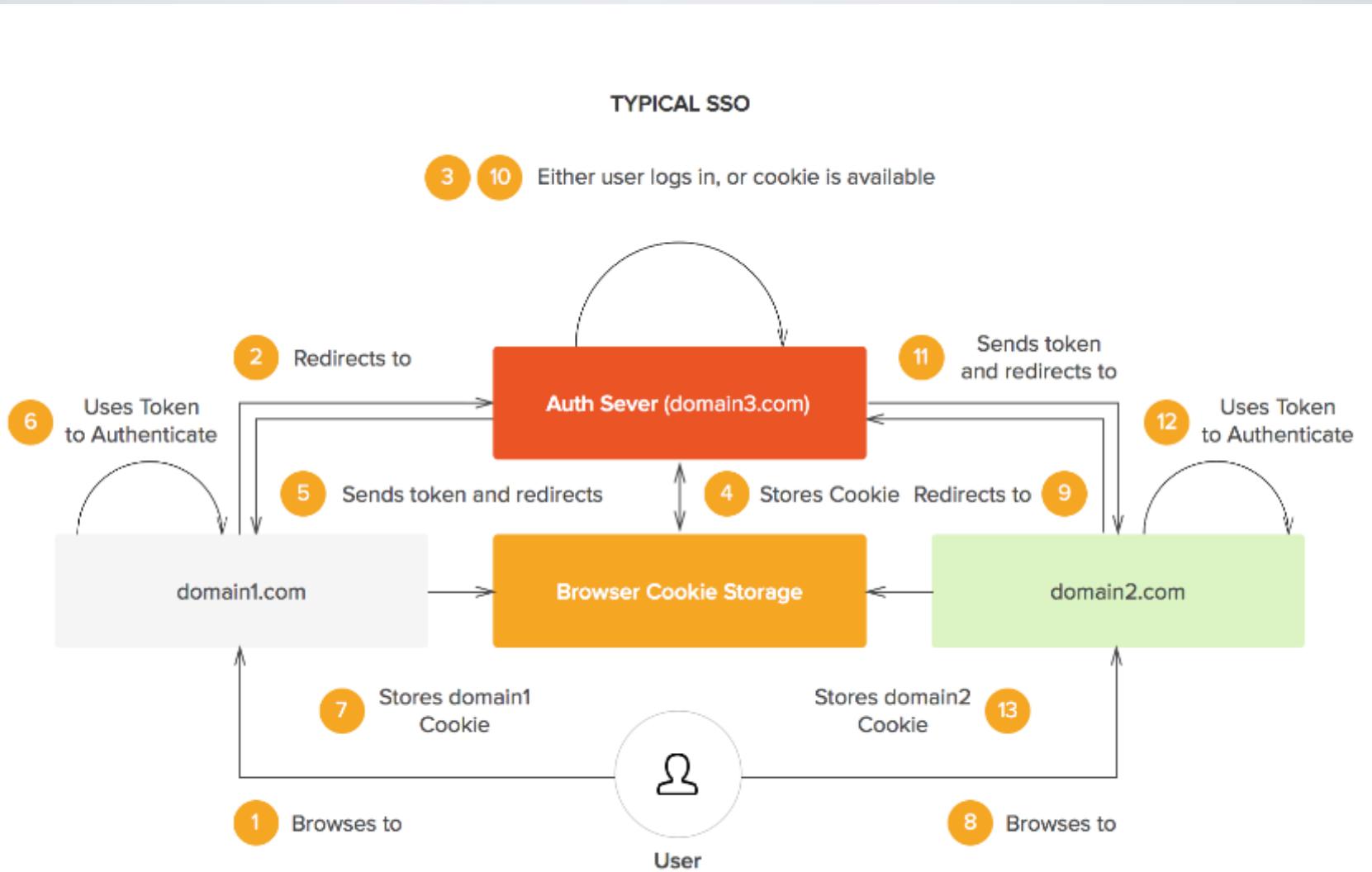


Share session information across different domains?

SAME-ORIGIN-POLICY FORBIDS THIS

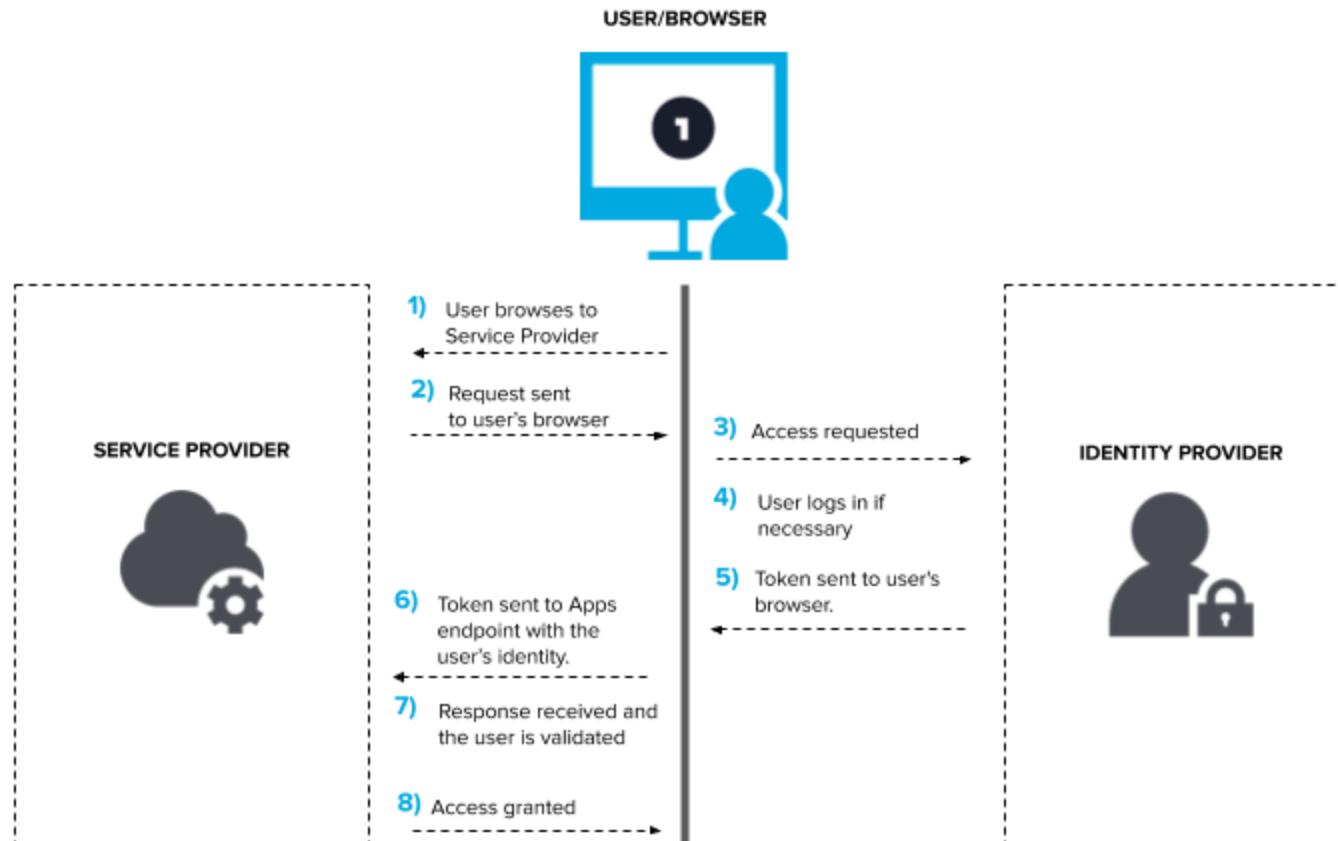


With Single Sign On



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?

- ➊ Traditional authentication tends to deliver full access in one go
 - secondary authentication sometimes required for specific applications or services
- ➋ 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

< LOCK SCREEN AND SECURITY

PHONE SECURITY

Screen lock type
PIN, Fingerprints

Smart Lock
Keep your phone unlocked when it's in a trusted location or detects a trusted device nearby.

Secure lock settings
Set your secure lock functions, such as Auto-lock and Lock instantly with Power key.

BIOMETRICS

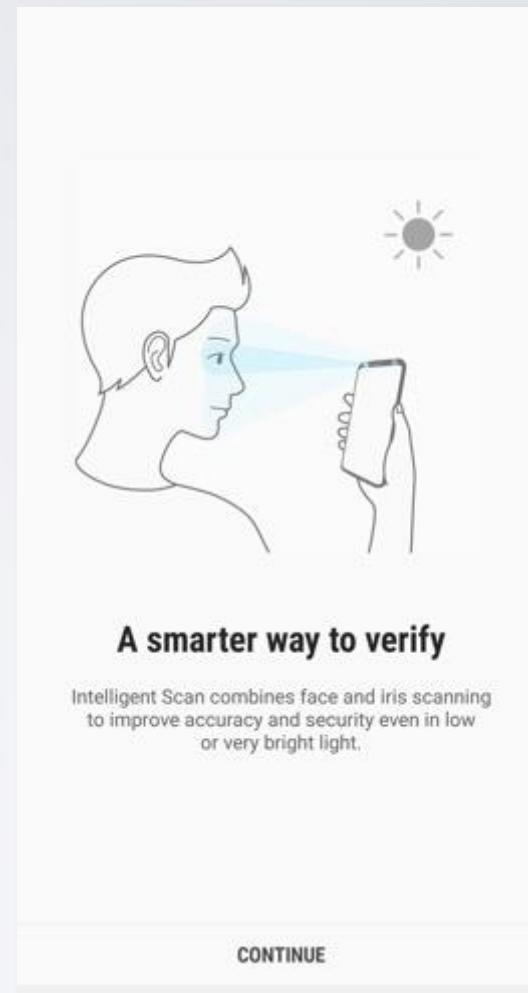
Intelligent Scan
Combined face and iris scanning for better results. Register your face and irises to use Intelligent Scan.

Face Recognition
Your face has been registered.

Iris Scanner
Register your irises.

Fingerprint Scanner
2 fingerprints have been added.

LOCK SCREEN AND ALWAYS ON DISPLAY



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)



Low value
asset
(Full access)



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

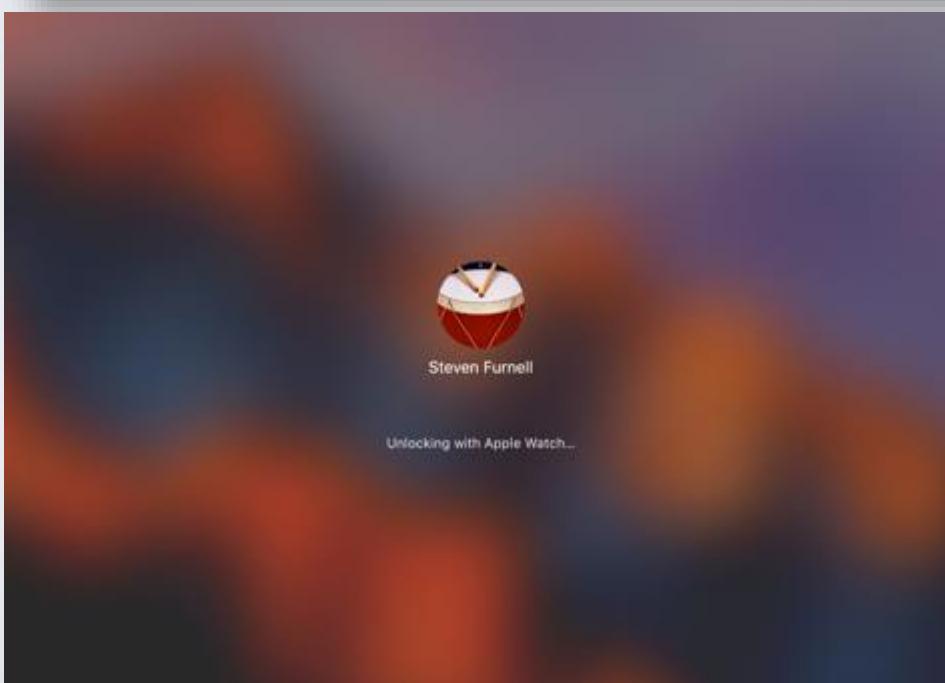
The strength of his Aura permits access to some devices but not others

Current Practice

A login password has been set for this user

[Change Password...](#)

- Require password 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



Mac Unlocked
"SMF MacBook Pro"
unlocked by this
Apple Watch

[Dismiss](#)

What is authorization?



Authorization/ Control access

- An identity permits access to resources
- Authorization limits a *subject's* access to 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

- ➊ The range of authentication options has grown
 - still no single solution that is universally applicable and effective
- ➋ 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

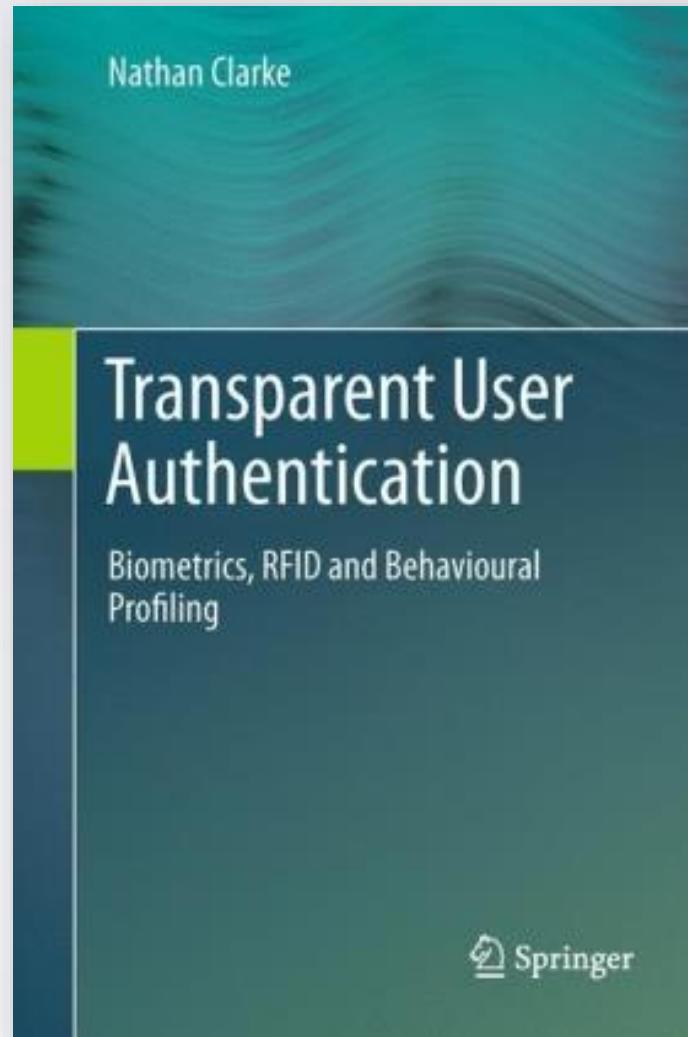


2-min paper

• 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 ...

iTunes U • Plymouth University

Networks & Security
Plymouth University
Description

The Centre for Security, Communications and Network Research is an established multidisciplinary group, applying academic expertise to the needs of industry and society. Themes within the Centre include information systems security, fraud, mobile & satellite communications and framework technologies.

#	Name	Released	Description	Popularity	Price
1	The Threat Landscape 2011	09/11	Simon Furnell introduces Ryan Horwood's work on the threat landscape for 2011.	10000+ (1)	£0.99
2	Managing mobile devices	09/11	A discussion of the IT and security management of mobile devices.	10000+ (1)	£0.99
3	Vulnerability management	02/11	Considering the essential role of vulnerability management.	10000+ (1)	£0.99
4	The evolving challenge of end-user security	07/11	A segment from the Networks talk delivered at the South West Cyber Security Conference.	10000+ (1)	£0.99
5	The CISO's Guide to Information Security	03/11	This file presents an invited talk to the South West Cyber Security Conference.	10000+ (1)	£0.99
6	Social networks - a case of viruses	02/11	An examination of the challenges that come from social networks.	10000+ (1)	£0.99
7	Strange things about human behaviour and security	09/11	This file presents the keynote presentation from the 2011 Security Awareness Conference.	10000+ (1)	£0.99
8	Cloud Security - Are we high in the clouds?	07/11	This file presents extracts from a panel discussion.	10000+ (1)	£0.99
9	Selecting Security Champions	03/11	Simon Furnell and Trevor Gabinet discuss the role of security champions.	10000+ (1)	£0.99
10	Regional Security Awareness	07/11	Extracts from a seminar presentation at the South West Cyber Security Conference.	10000+ (1)	£0.99
11	Transparent versus explicit security	02/11	Extracts from a seminar examining the balance between transparency and explicitness.	10000+ (1)	£0.99
12	00 - Multi-Level Logon 2	01/11	This is the ninth of a series of videos that introduce multi-level logons.	10000+ (1)	£0.99
13	00 - Multi-Level Logon 1	01/11	This is the eighth of a series of videos that introduce multi-level logons.	10000+ (1)	£0.99
14	07 - Basic Authentication	01/11	This is the seventh of a series of videos that introduce basic authentication.	10000+ (1)	£0.99
15	06 - Remote Admin Access	01/11	This is the sixth of a series of videos that introduce remote admin access.	10000+ (1)	£0.99

Filter by items



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