School of Computing
FACULTY OF ENGINEERING & PHYSICAL SCIENCES

UNIVERSITY OF LEEDS

COMP3911 Secure Computing

7: User Authentication

Nick Efford

https://comp3911.info

Objectives

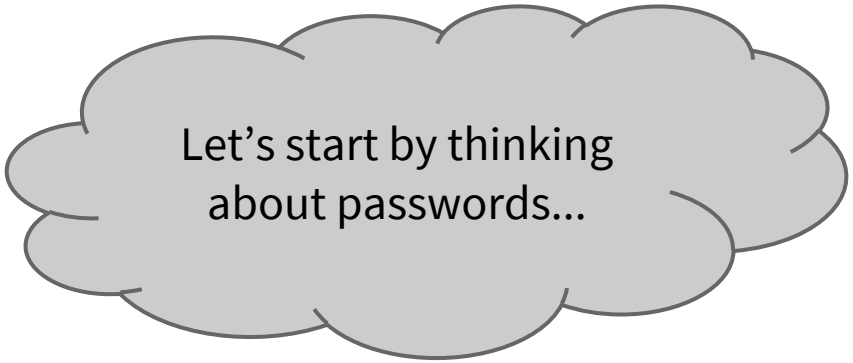
UNIVERSITY OF LEEDS

- For you to recognise the main approaches that exist for **user authentication**
- For you to understand the theoretical and practical levels of security achievable with passwords
- For you to appreciate the benefits and limitations of security tokens and biometrics

Basis For Authentication

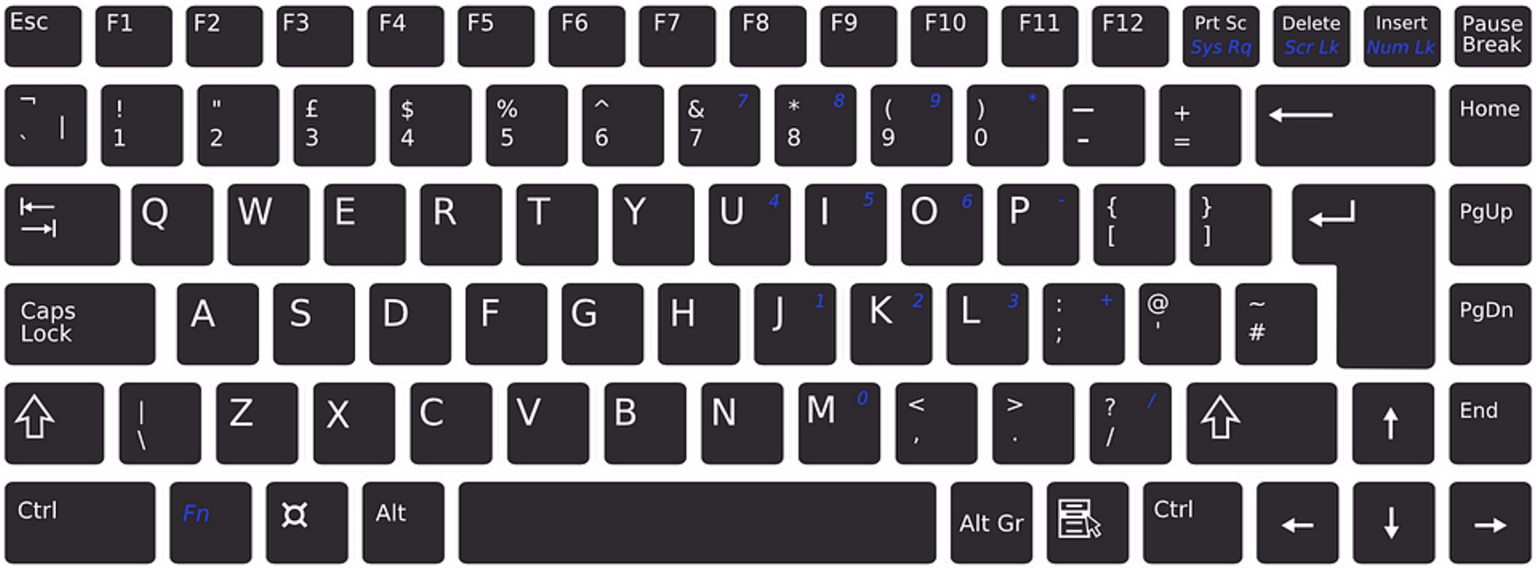
UNIVERSITY OF LEEDS

- “Something you know”
  - PIN, password, passphrase
- “Something you have”
  - Physical security token (key, smartcard…)
- “Something you are”
  - Biometric measurement



How Many Passwords?

UNIVERSITY OF LEEDS

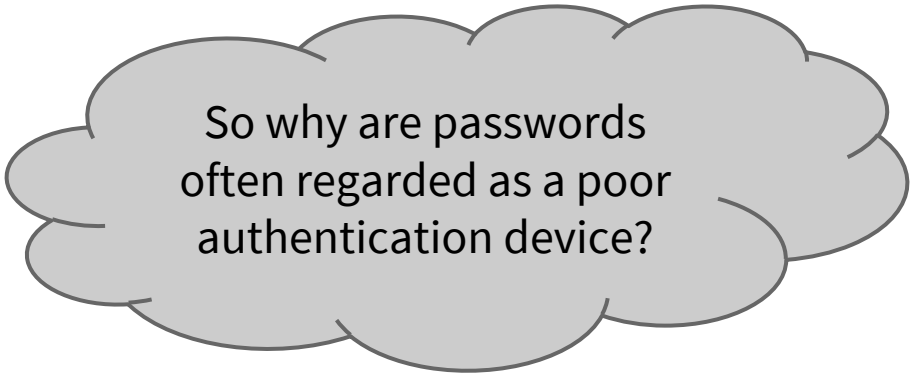


1. Write an expression for the number of possible passwords of length *L*, given that *N* different characters can be typed
2. Estimate *N* for a typical keyboard and evaluate this expression for eight-character passwords

Solution

UNIVERSITY OF LEEDS

- If there are N unique characters that can be typed
- … and a password consists of L characters
- … then there are N^L possible passwords!
- $N \approx 95$ for UK keyboard (ignoring 'special characters')
- … So if $L = 8$ there are 95^8 possible passwords
- … i.e., roughly 6.6 quintillion! (6.6×10^{15})



Entropy (Again)

UNIVERSITY OF LEEDS

For the previous scenario:

Total entropy $= \log_2 N^L = \log_{10} N^L / \log_{10} 2 = 52.56$ bits

$\Rightarrow$ Entropy per character = **6.57 bits**

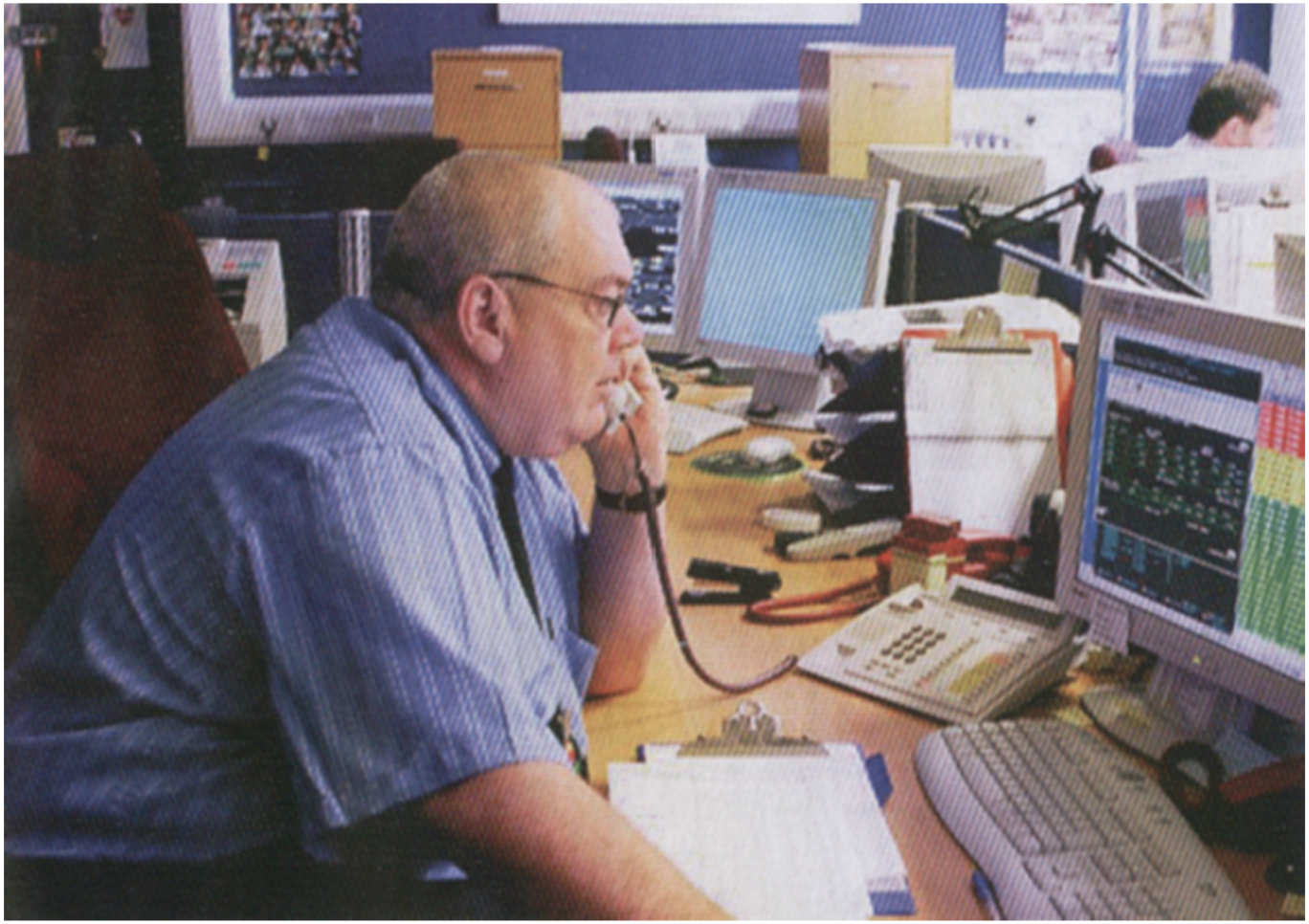
Compare: Entropy per letter for English $\approx$ **1.8 bits**

What is the entropy of a 4-digit PIN?

1. In general
2. For the keypad on the right

2005: GNER Control Centre

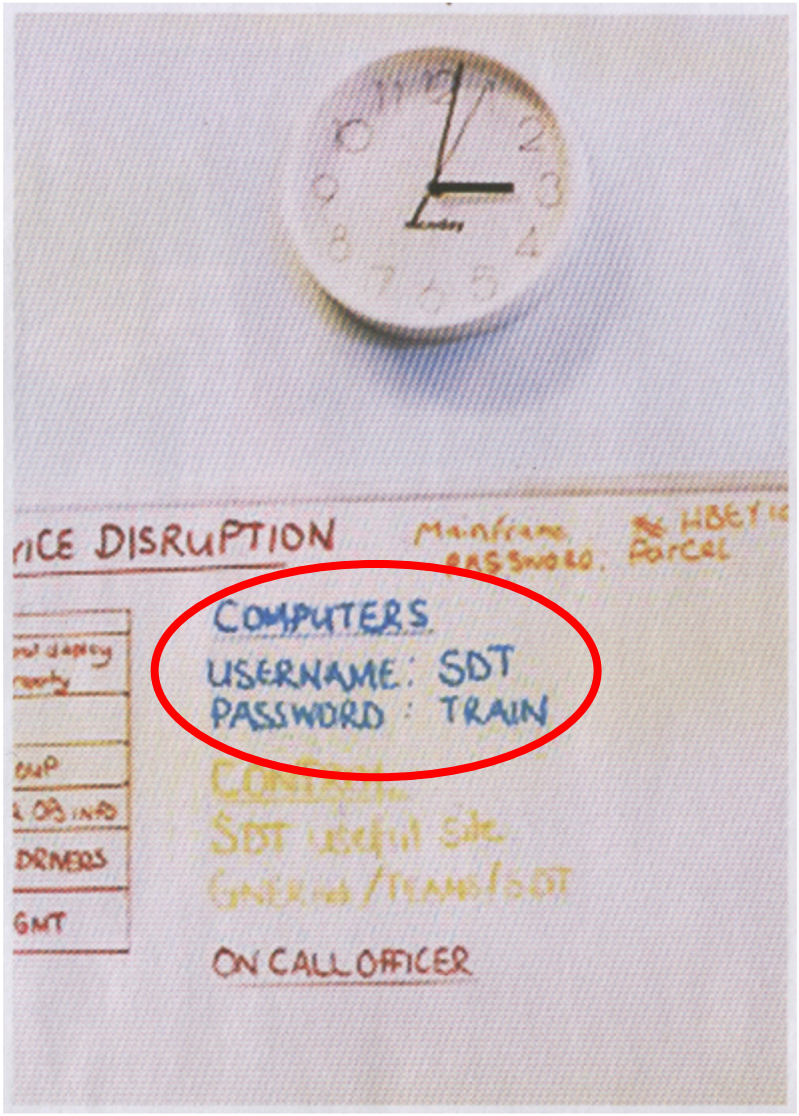
UNIVERSITY OF LEEDS



(Scanned from *LiveWire* magazine, April/May issue)

2005: GNER Control Centre

UNIVERSITY OF LEEDS



2014: Winter Floods

UNIVERSITY OF LEEDS

(Screen grab from Sky News)

2015: Waterloo Station

UNIVERSITY OF LEEDS

(Screen grab from a BBC2 documentary)

2016: Labour Leadership Contest

UNIVERSITY OF LEEDS

(Posted on Twitter by Owen Smith's campaign staff)

2018: Trump Administration

UNIVERSITY OF LEEDS

The committee may also consider adding ProtonMail, the encrypted email service, to that list. One White House staffer, Ryan P. McAvoy, jotted his ProtonMail passwords and his address on a piece of White House stationery and left it at a bus stop near the White House. A source found it there and provided it to The Intercept, which confirmed its authenticity. (McAvoy did not respond to requests for comment.)

Following publication of this story, Irina Marcopol, a spokesperson for ProtonMail, forwarded a statement from the company's CEO, Andy Yen. "Don't be a password idiot," Yen suggested. "In other words, don't be this guy."

https://theintercept.com/2018/03/17/trump-russia-apple-whatsapp/

Conclusions

UNIVERSITY OF LEEDS

- Humans sample a very small region of ‘password space’
- … and they write passwords down
- … and let others see them

Other Risks

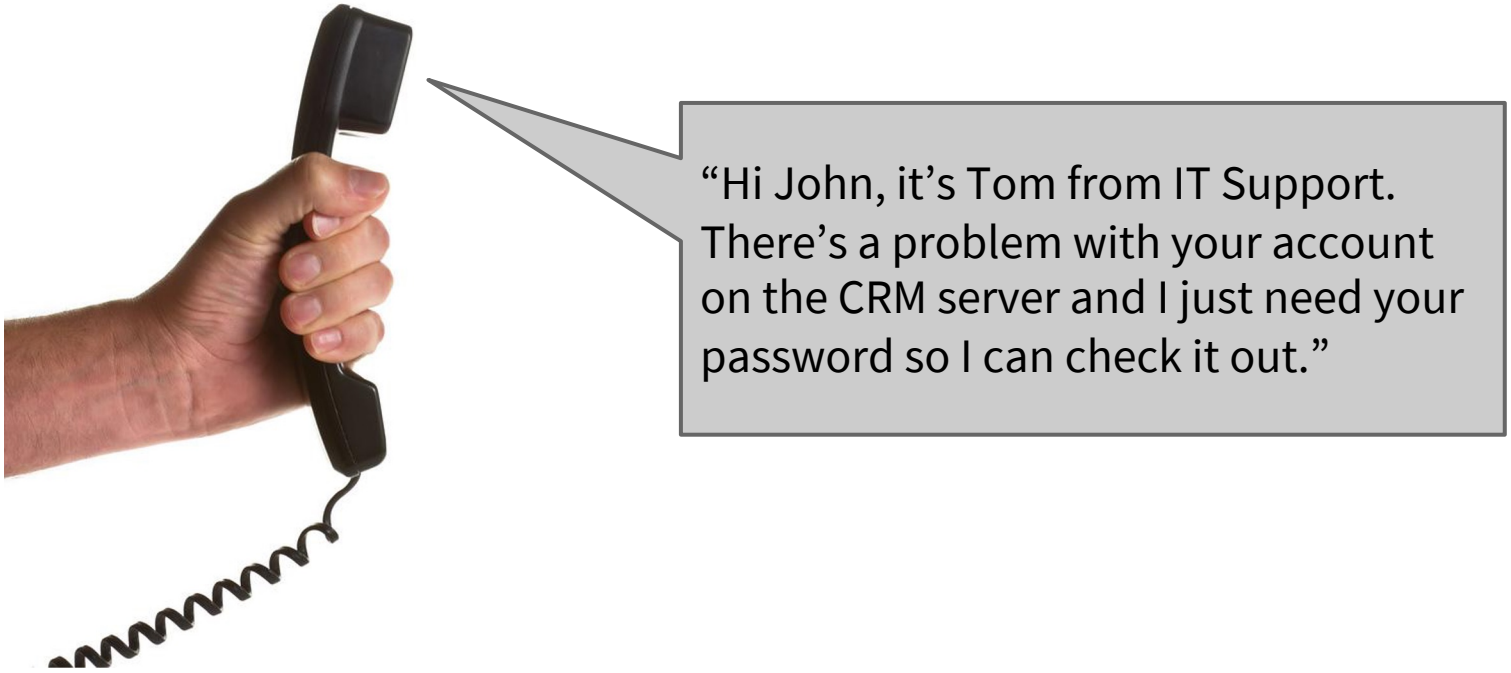
UNIVERSITY OF LEEDS

- Factory defaults
- ‘Shoulder surfing’
- Social engineering
- Keystroke loggers / Trojans
- Live brute-forcing
- Cracking of stolen hashes
- Information leakage in system logs

Social Engineering

UNIVERSITY OF LEEDS

- Done on a large scale these days via **phishing**
- More targeted attacks may involve direct communication with an individual…



KeySweeper

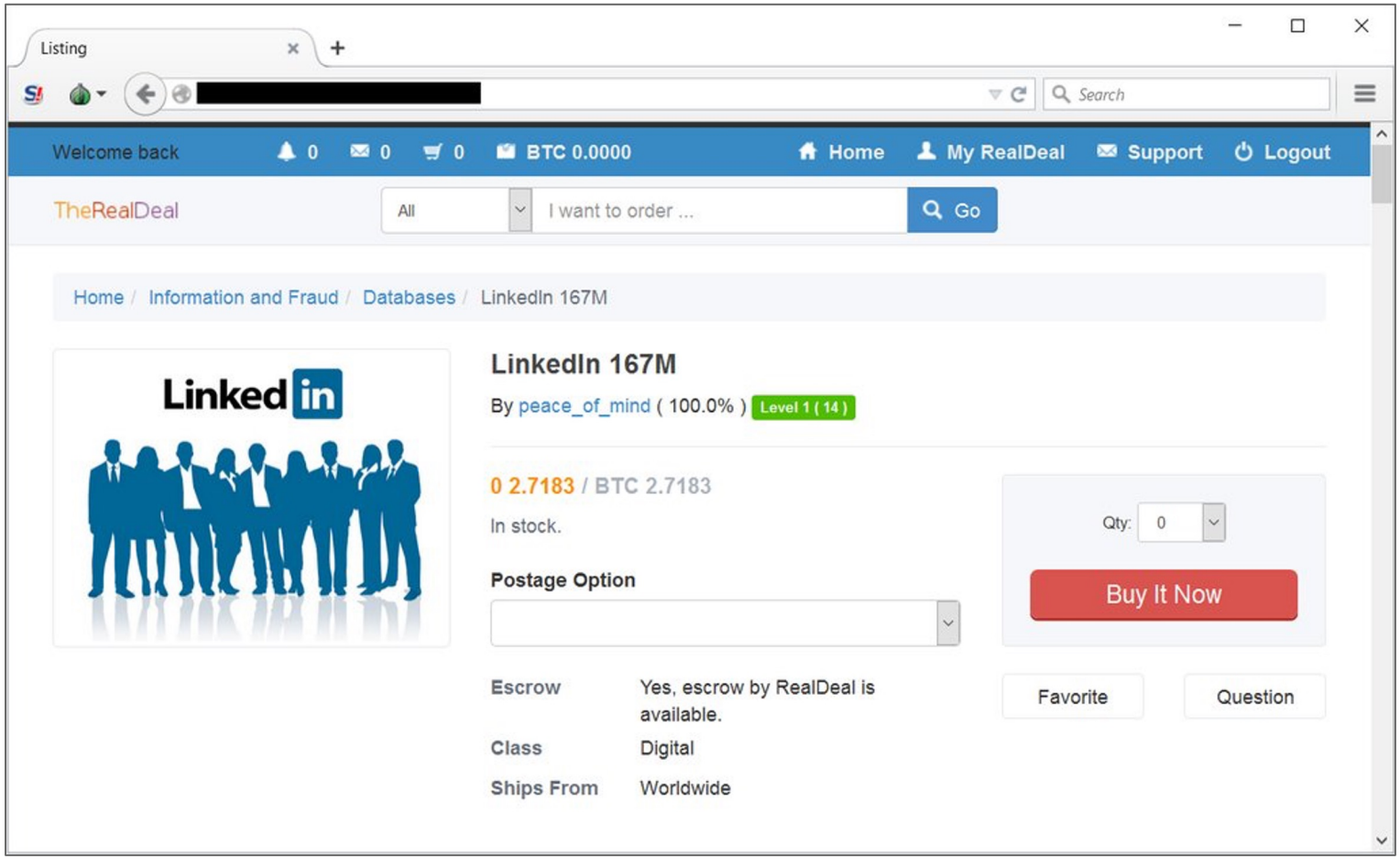
UNIVERSITY OF LEEDS

- Looks like a phone charger
- Sniffs keystrokes for certain Microsoft wireless keyboards and logs them on the device
- Can detect usernames and passwords and send them to attacker via SMS

Cracking Stolen Hashes

UNIVERSITY OF LEEDS

Credentials are stolen in data breaches and then sold…



Password Hashing

UNIVERSITY OF LEEDS

- Store a hash of a password, not password itself!
- **Problem 1**: hash functions are fast by design, so live brute-forcing would be efficient
  - Solution: **slow down hashing** by iterating a large number of times
- **Problem 2**: attacker could precompute a mapping of hashes onto passwords, for a range of password choices
  - Solution: choose **random salt** s, compute $H(p \,||\, s)$, and store salt and hash in the database
  - Attacker now needs to precompute mappings for all possible combinations of p and s!

Hash Cracking Algorithm

UNIVERSITY OF LEEDS

For each user u in stolen file:

Read hash h and salt s for the user

For each word w in a word list:

Generate a set of variations, $w_1 \ldots w_n$

For each variation w_i:

Compute $h^* \longleftarrow H(w_i \,||\, s)$

If $h^* = h$, record w_i as password of u

In past studies, this consistently cracks 20–35% of passwords!

Physical Tokens & 2FA

UNIVERSITY OF LEEDS

- Passwords are cheap and convenient, but relatively weak as an authentication device
- Simple way of strengthening auth is to combine them with a physical token, in **two-factor authentication** (2FA)
- Examples: mobile phone, smartcard, YubiKey

Key acts like a USB keyboard; touching the button generates a character sequence that is used as a **one-time password**

Biometrics

UNIVERSITY OF LEEDS

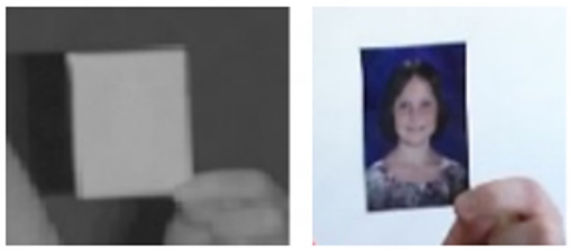
- Potentially the most convenient for users
- Can be expensive to implement
- Many traits to choose from
  - Voice
  - Fingerprints
  - Facial geometry
  - Eye features
    - Retinal blood vessels
    - Iris texture

Some Examples

UNIVERSITY OF LEEDS

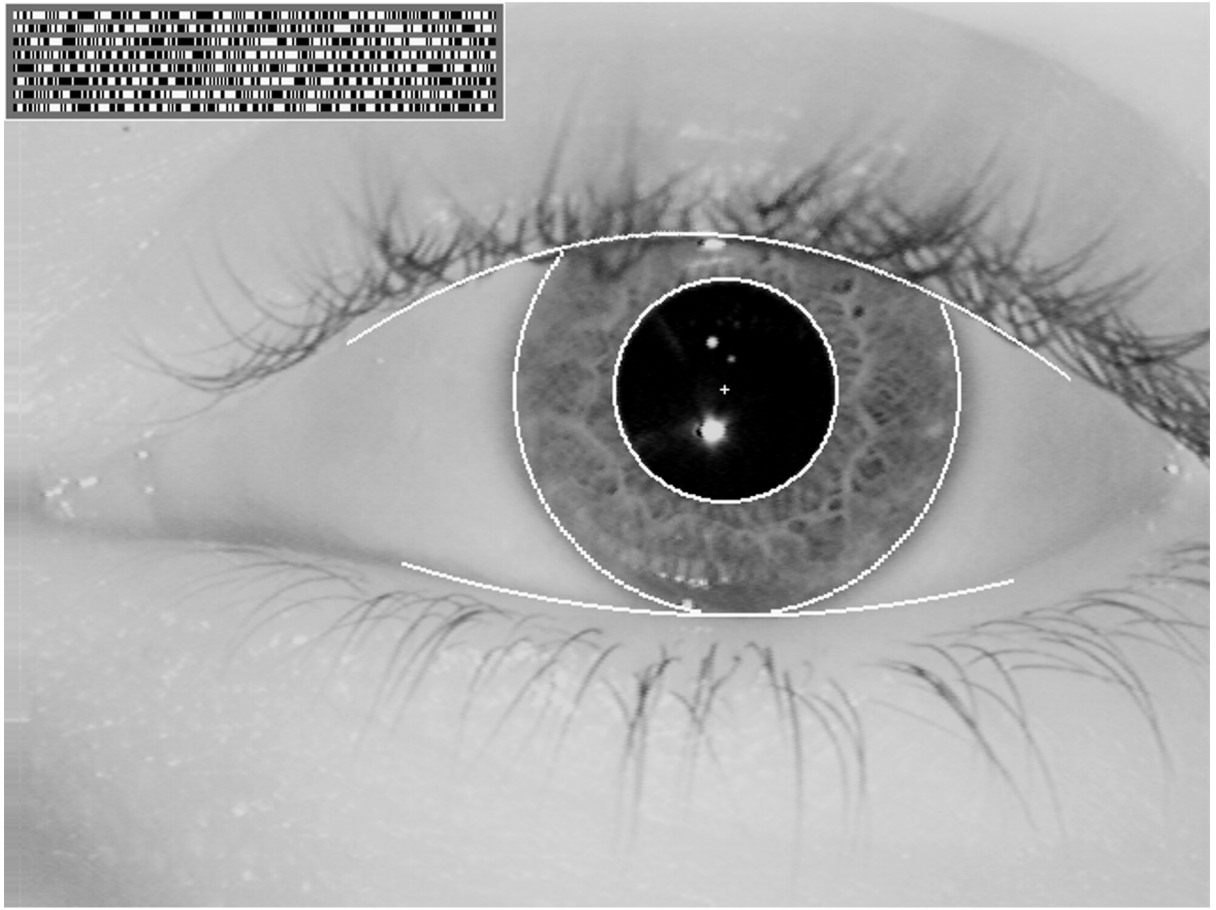
- Face recognition in ‘Windows Hello’
  - Uses Near-IR images
  - Samples texture around landmark points
  - Can use depth sensors if available
- Apple’s FaceID & TouchID

NIR vs visible light



Iris Codes

UNIVERSITY OF LEEDS



Being used by Indian government for its 1.2 billion citizens, and in Microsoft's Lumia 950 phone...

The Revocation Problem

UNIVERSITY OF LEEDS

- If a database of biometric credentials were compromised, what could we do? Biometrics are irrevocable!
- Solution is to combine a revocable factor with a biometric factor, hash this and store the hash
    - Can revoke the hash and change the revocable factor if the database is subsequently hacked

Eyeball replacement is not an option!

Summary

UNIVERSITY OF LEEDS

We have

- Seen that, although the space of possible passwords is typically quite large, passwords are often poorly-chosen / written down by users
- Discussed a range of other password-related risks
- Considered how easy it is to crack stolen password hashes
- Noted that 2FA strengthens password authentication by combining it with a physical token
- Examined some popular biometric techniques

Follow-Up / Further Reading

UNIVERSITY OF LEEDS

- Exercise 11, on password hashing
- Exercise 12, covering the John the Ripper and Hydra password cracking tools
- KeySweeper video (YouTube)
- DataBreaches.net: reports on the latest breaches
- Have I Been Pwned (HIBP): check if you have an account that has been compromised in a data breach
- Strong two-factor authentication with YubiKey
- BioStar 2 biometric data breach (Aug 2019)