# CT255
# Introduction to Cybersecurity

## Lecture 3

## Human Security - Passwords

Dr. Michael Schukat, 2021-22

# Background and Lecture Overview

- Security is only as good as its weakest link, and in many organisations this link is the human factor
- In today’s lecture we’ll study different authentication methodologies, including passwords, and their inherent weaknesses

# Learning Outcomes

- You’ll be able to:
  - Distinguish between different authentication methods, their strengths and weaknesses
  - Explore strategies to predict user passwords

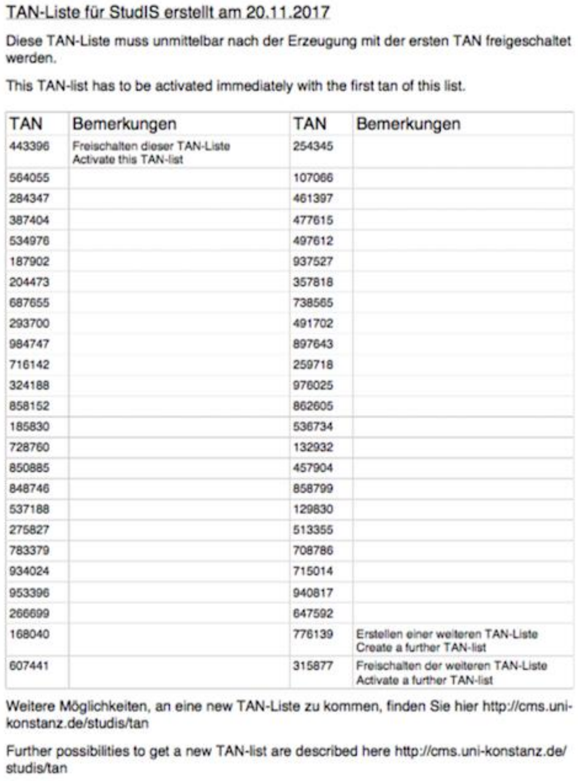
# What is a Password?

- A memorized secret used to confirm the identity of a user
  - Typically an arbitrary string of characters including letters, digits, or other symbols
  - A purely numeric secret is called a personal identification number (PIN)
- The secret is memorized by a party called the **claimant** while the party verifying the identity of the claimant is called the **verifier**
- Claimant and verifier communicate via an **authentication protocol**

# Some Password Alternatives

- One-time password (OTP)
  - Transaction authentication number (TAN) list used for online banking – they can only be used once
- Time-synchronized one-time passwords
- Biometric methods
  - fingerprints, irises, voice, face
- Cognitive passwords
  - Use question and answer cue/response pairs to verify identity

# Examples for TAN Lists



TAN-Liste für StudIS erstellt am 20.11.2017

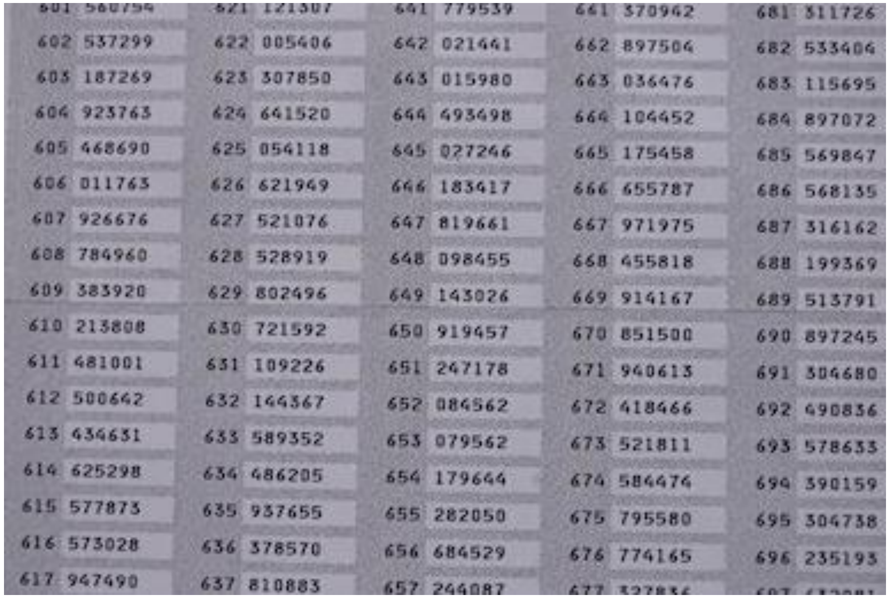
Diese TAN-Liste muss unmittelbar nach der Erzeugung mit der ersten TAN freigeschaltet werden.

This TAN-list has to be activated immediately with the first tan of this list.

| TAN | Bemerkungen | TAN | Bemerkungen |
|---|---|---|---|
| 443396 | Freischalten dieser TAN-Liste<br>Activate this TAN-list | 254345 | |
| 564055 | | 107066 | |
| 284347 | | 461397 | |
| 387404 | | 477615 | |
| 534976 | | 497612 | |
| 187902 | | 937527 | |
| 204473 | | 357818 | |
| 687655 | | 738565 | |
| 293700 | | 491702 | |
| 984747 | | 897643 | |
| 716142 | | 259718 | |
| 324188 | | 976025 | |
| 858152 | | 862605 | |
| 185830 | | 536734 | |
| 728760 | | 132932 | |
| 850885 | | 457904 | |
| 848746 | | 858799 | |
| 537188 | | 129830 | |
| 275827 | | 513355 | |
| 783379 | | 708786 | |
| 934024 | | 715014 | |
| 953396 | | 940817 | |
| 266699 | | 647592 | |
| 168040 | | 776139 | Erstellen einer weiteren TAN-Liste<br>Create a further TAN-list |
| 607441 | | 315877 | Freischalten der weiteren TAN-Liste<br>Activate a further TAN-list |

Weitere Möglichkeiten, an eine new TAN-Liste zu kommen, finden Sie hier http://cms.uni-konstanz.de/studis/tan

Further possibilities to get a new TAN-list are described here http://cms.uni-konstanz.de/studis/tan



| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 601 | 560754 | 621 | 121307 | 641 | 779539 | 661 | 370942 | 681 | 311726 |
| 602 | 537299 | 622 | 005406 | 642 | 021441 | 662 | 897504 | 682 | 533404 |
| 603 | 187269 | 623 | 307850 | 643 | 015980 | 663 | 036476 | 683 | 115695 |
| 604 | 923763 | 624 | 641520 | 644 | 493498 | 664 | 104452 | 684 | 897072 |
| 605 | 468690 | 625 | 054118 | 645 | 027246 | 665 | 175458 | 685 | 569847 |
| 606 | 011763 | 626 | 621949 | 646 | 183417 | 666 | 655787 | 686 | 568135 |
| 607 | 926676 | 627 | 521076 | 647 | 819661 | 667 | 971975 | 687 | 316162 |
| 608 | 784960 | 628 | 528919 | 648 | 098455 | 668 | 455818 | 688 | 199369 |
| 609 | 383920 | 629 | 802496 | 649 | 143026 | 669 | 914167 | 689 | 513791 |
| 610 | 213808 | 630 | 721592 | 650 | 919457 | 670 | 851500 | 690 | 897245 |
| 611 | 481001 | 631 | 109226 | 651 | 247178 | 671 | 940613 | 691 | 304680 |
| 612 | 500642 | 632 | 144367 | 652 | 084562 | 672 | 418466 | 692 | 490836 |
| 613 | 434631 | 633 | 589352 | 653 | 079562 | 673 | 521811 | 693 | 578633 |
| 614 | 625298 | 634 | 486205 | 654 | 179644 | 674 | 584476 | 694 | 390159 |
| 615 | 577873 | 635 | 937655 | 655 | 282050 | 675 | 795580 | 695 | 304738 |
| 616 | 573028 | 636 | 378570 | 656 | 684529 | 676 | 774165 | 696 | 235193 |
| 617 | 947490 | 637 | 810883 | 657 | 244087 | 677 | 327836 | 697 | [illegible] |

# Algorithmic Generation of OTP

- Paper-based TANs are hard to manage
- On the other hand both claimant and verifier need to have a copy of every OTP (possibly hundreds of them)
- Idea: Each new OTP may be created from the past OTPs used
- An example of this type of algorithm, credited to Leslie Lamport, uses a one-way function (hash function)

# One-Way Functions

- A one-way function $H$ produces a fixed-size output $h$ based on a variable size input $s$
  - $H(s) = h$
  - $H$ is also called a hash function, $h$ is called a hash (value)
  - Example:
    $H$(“KenSentMe!”) = “7b24afc8bc80e548d66c4e7ff72171c5”
- Important: **One way property**:
  For a given hash code $h$ it is infeasible to find $s$ that $H(s) = h$

# Leslie Lamport’s Algorithm

- For every claimant a random seed (starting value) s is chosen
- A hash function H(s) is applied repeatedly (for example, 1000 times) to the seed, giving a value of: H(H(H( .... H(s) ....)))
- This value, also called $H^{1000}(s)$, is stored by the verifier
- The claimant keeps the seed s

# Leslie Lamport’s Algorithm

- The user's first login uses an OTP $p$ derived by applying $H$ 999 times to the seed, i.e. $H^{999}(s)$)
- The verifier can authenticate that this is the correct OTP, because $H(p) = H^{1000}(s)$, the value stored
- The value stored is then replaced by $p$ and the user is allowed to log in

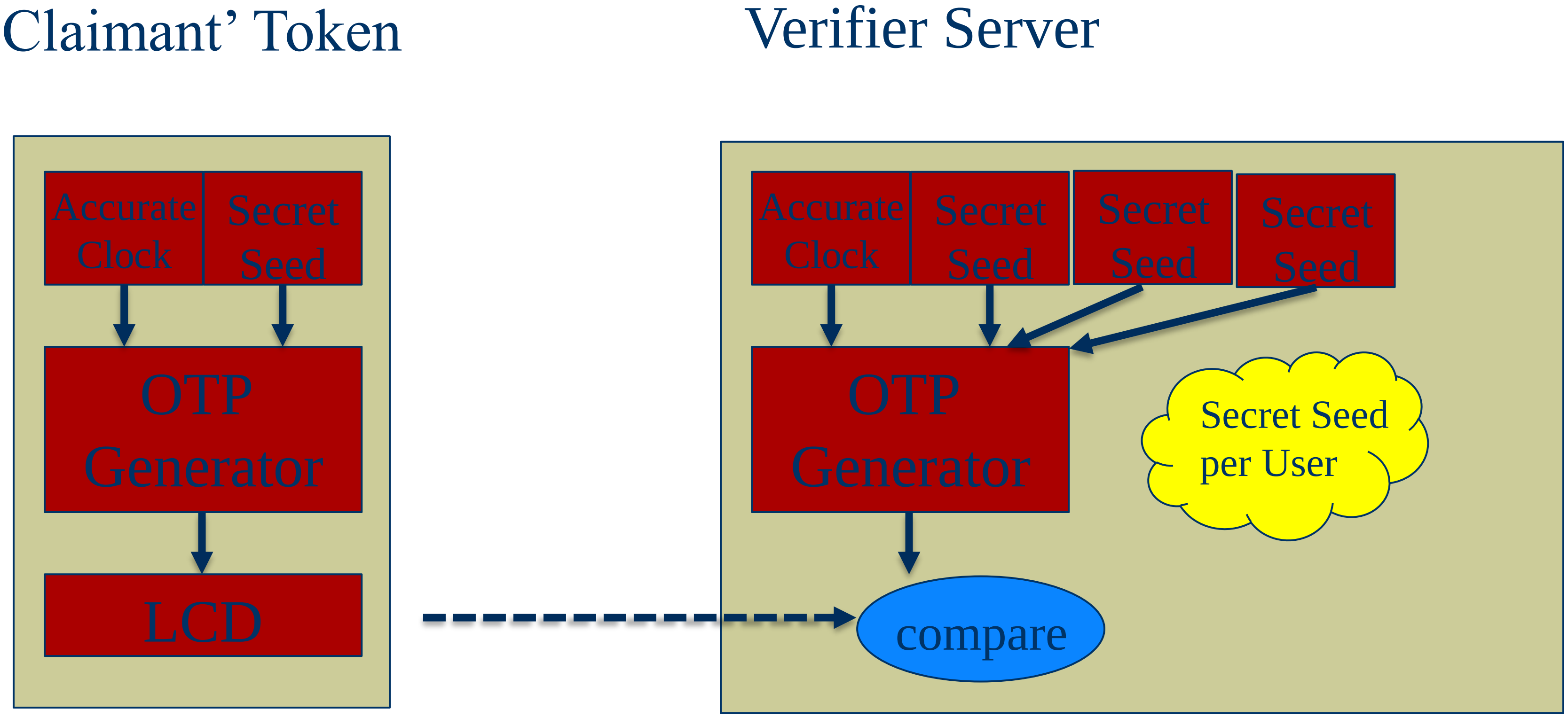
# Leslie Lamport's Algorithm

- The next login must be accompanied by $H^{998}(s)$
- Again, this can be validated because hashing gives $H^{999}(s)$ which is $p$, the value stored after the previous login
- The new value replaces $p$ and the user is authenticated
- This process can be repeated another 997 times, each time the password will be $H$ applied one fewer times

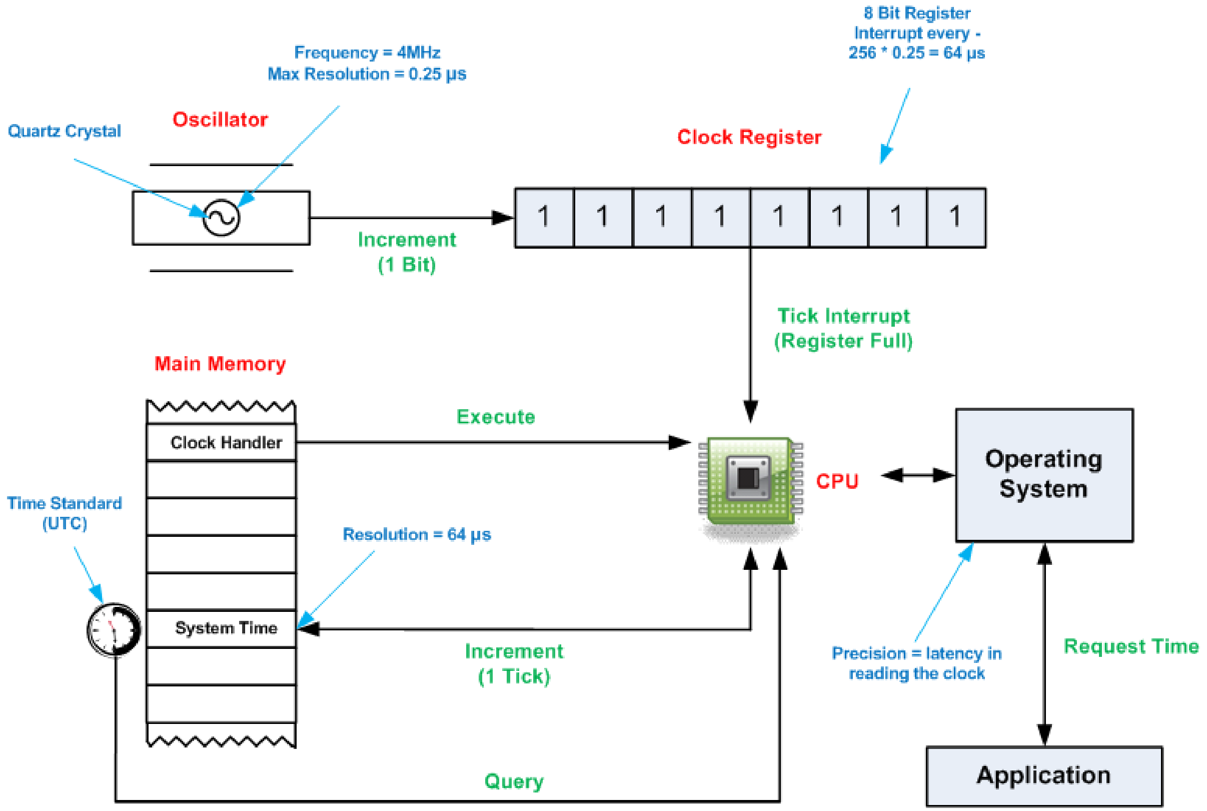
# Time-synchronised OTP

- Each user has a unique piece of hardware called a security token that generates an OTP (e.g. mobile phone or gadget with LCD)
- Inside the token is an accurate clock that has been synchronized with the clock of the verifier
- Both claimant token and verifier server calculate identical OPTs that are based on time

# Time-synchronised OTP



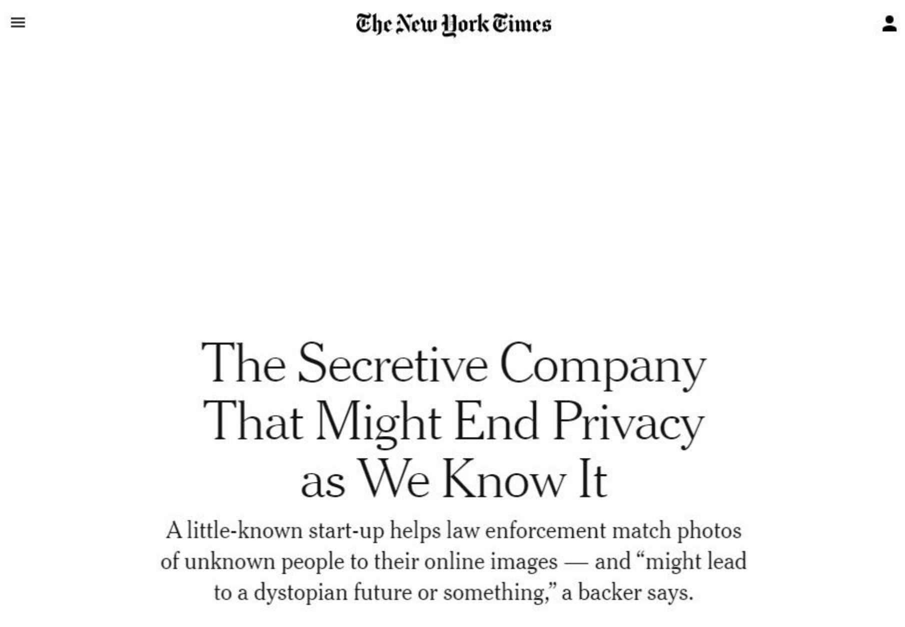
# Problem here: An accurate Token Clock



# Some new Biometric Methods

- Hand geometry
  Measurement and comparison of the (unique) different physical characteristics of the hand
- Palm vein authentication
  Uses an infrared beam to penetrate the users hand as it is waved over the system; the veins within the palm of the user are returned as black lines
- Retina scan
  Provides an analysis of the capillary blood vessels located in the back of the eye
- Iris scan
  Provides an analysis of the rings, furrows and freckles in the colored ring that surrounds the pupil of the eye
- Face recognition, signature and voice analysis

# NYT Article (18/01/20) about Start-Up Company Clearview AI


The New York Times

The Secretive Company That Might End Privacy as We Know It

A little-known start-up helps law enforcement match photos of unknown people to their online images — and "might lead to a dystopian future or something," a backer says.

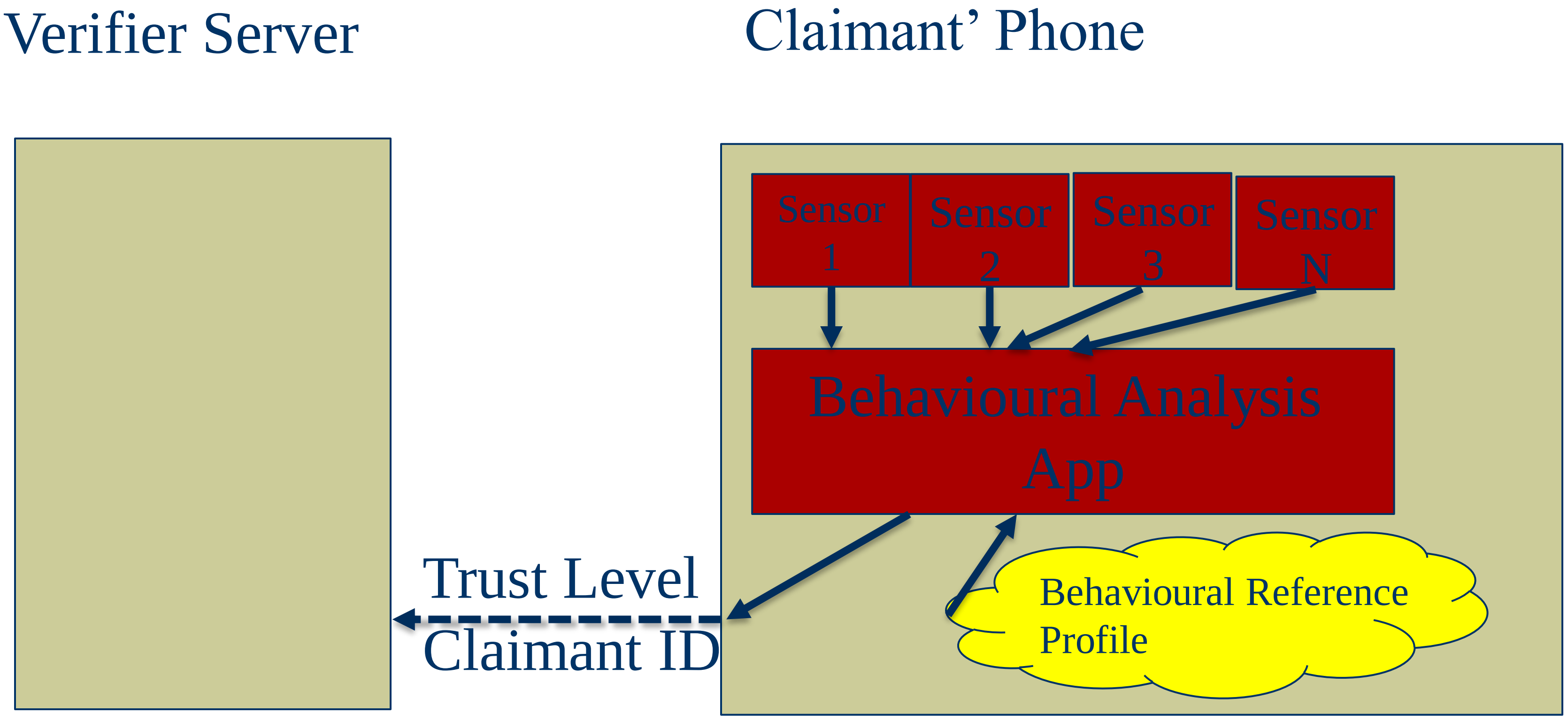
# Reclaim your Face

- https://reclaimyourface.eu/
- https://reclaimyourface.eu/how-to-reclaim-your-face-from-clearview-ai/

# The Pitfalls of Biometrics

- https://www.youtube.com/watch?v=ZPG3XQhZVII
- Please watch!

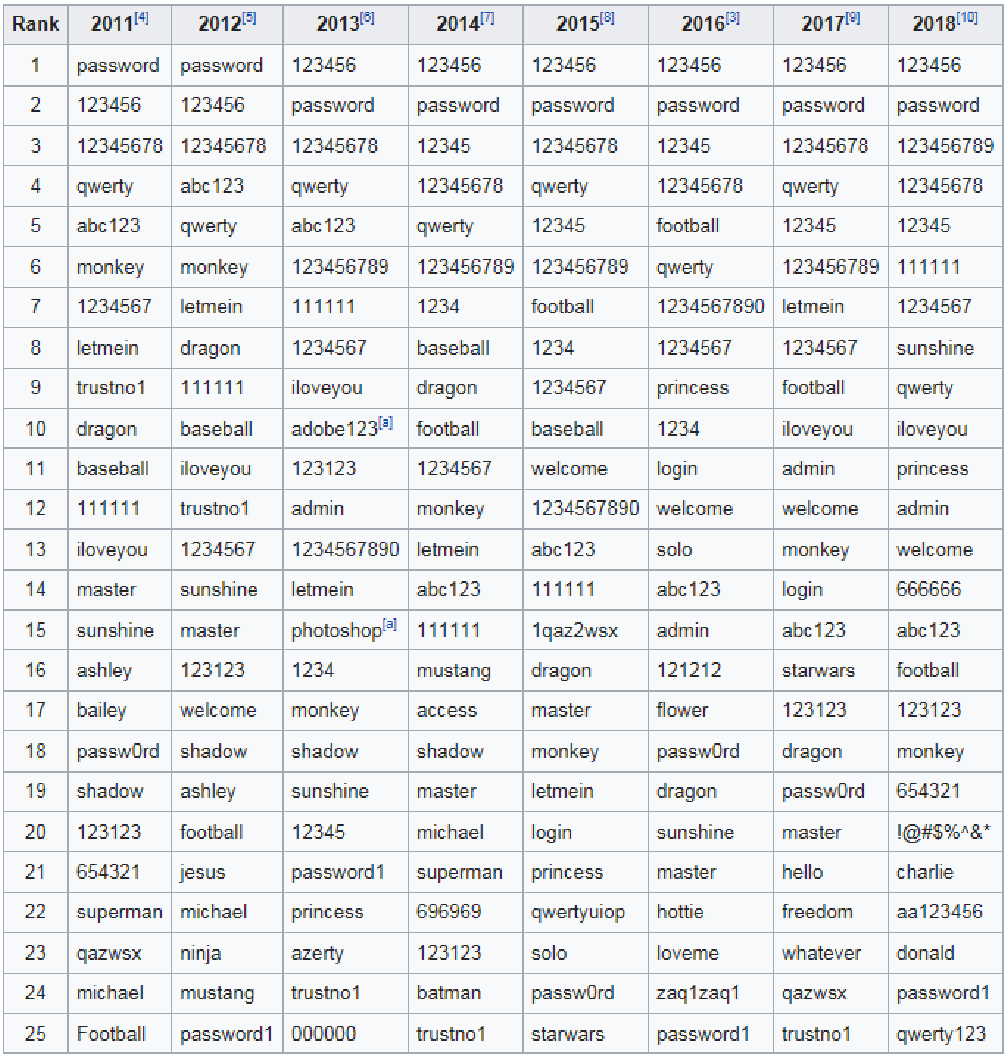
# Behavioural Biometrics



# Multi-Factor Authentication

- This may include a combination of the following:
  - Some physical object in the possession of the user, e.g. a USB stick with a secret token, a bank card, a key, etc.
  - Some secret known to the user, such as a password, PIN, TAN, etc.
  - Some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.
  - Somewhere you are, such as connection to a specific computing network or utilizing a GPS signal to identify the location

# Most common passwords according to Internet Security Company SplashData



| Rank | 2011[4] | 2012[5] | 2013[6] | 2014[7] | 2015[8] | 2016[3] | 2017[9] | 2018[10] |
|---|---|---|---|---|---|---|---|---|
| 1 | password | password | 123456 | 123456 | 123456 | 123456 | 123456 | 123456 |
| 2 | 123456 | 123456 | password | password | password | password | password | password |
| 3 | 12345678 | 12345678 | 12345678 | 12345 | 12345678 | 12345 | 12345678 | 123456789 |
| 4 | qwerty | abc123 | qwerty | 12345678 | qwerty | 12345678 | qwerty | 12345678 |
| 5 | abc123 | qwerty | abc123 | qwerty | 12345 | football | 12345 | 12345 |
| 6 | monkey | monkey | 123456789 | 123456789 | 123456789 | qwerty | 123456789 | 111111 |
| 7 | 1234567 | letmein | 111111 | 1234 | football | 1234567890 | letmein | 1234567 |
| 8 | letmein | dragon | 1234567 | baseball | 1234 | 1234567 | 1234567 | sunshine |
| 9 | trustno1 | 111111 | iloveyou | dragon | 1234567 | princess | football | qwerty |
| 10 | dragon | baseball | adobe123[a] | football | baseball | 1234 | iloveyou | iloveyou |
| 11 | baseball | iloveyou | 123123 | 1234567 | welcome | login | admin | princess |
| 12 | 111111 | trustno1 | admin | monkey | 1234567890 | welcome | welcome | admin |
| 13 | iloveyou | 1234567 | 1234567890 | letmein | abc123 | solo | monkey | welcome |
| 14 | master | sunshine | letmein | abc123 | 111111 | abc123 | login | 666666 |
| 15 | sunshine | master | photoshop[a] | 111111 | 1qaz2wsx | admin | abc123 | abc123 |
| 16 | ashley | 123123 | 1234 | mustang | dragon | 121212 | starwars | football |
| 17 | bailey | welcome | monkey | access | master | flower | 123123 | 123123 |
| 18 | passw0rd | shadow | shadow | shadow | monkey | passw0rd | dragon | monkey |
| 19 | shadow | ashley | sunshine | master | letmein | dragon | passw0rd | 654321 |
| 20 | 123123 | football | 12345 | michael | login | sunshine | master | !@#$%^&* |
| 21 | 654321 | jesus | password1 | superman | princess | master | hello | charlie |
| 22 | superman | michael | princess | 696969 | qwertyuiop | hottie | freedom | aa123456 |
| 23 | qazwsx | ninja | azerty | 123123 | solo | loveme | whatever | donald |
| 24 | michael | mustang | trustno1 | batman | passw0rd | zaq1zaq1 | qazwsx | password1 |
| 25 | Football | password1 | 000000 | trustno1 | starwars | password1 | trustno1 | qwerty123 |

Source: Wikipedia

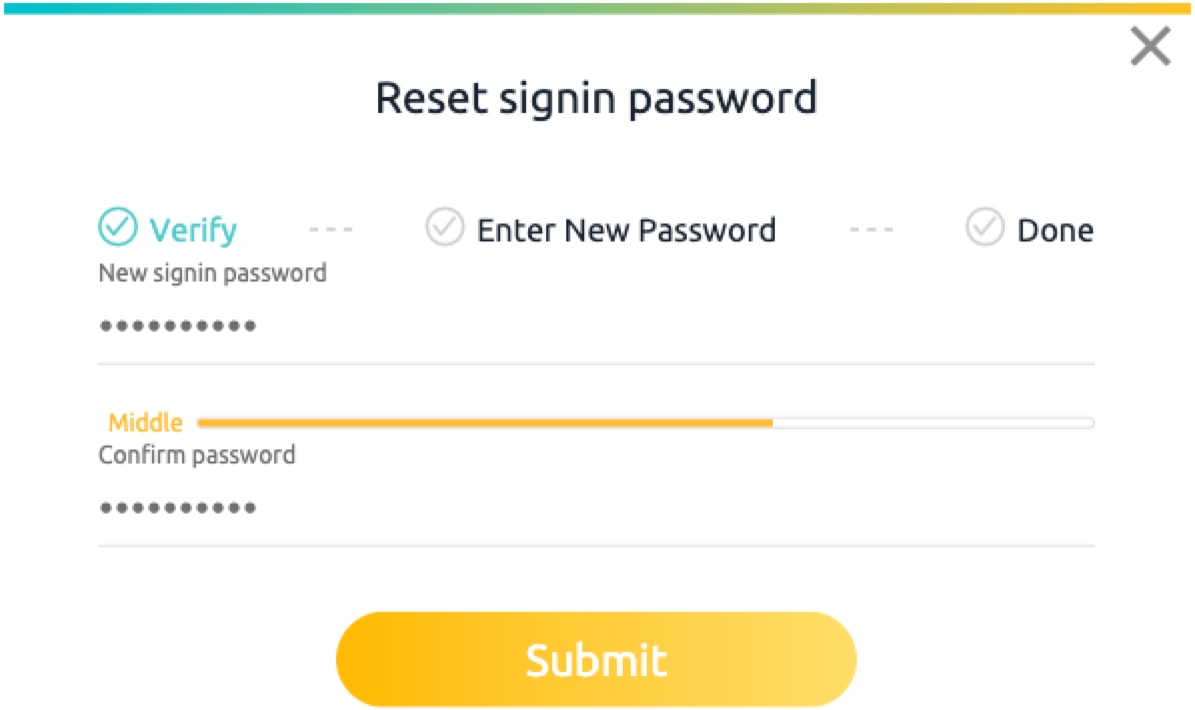
ty

NUI Galway
OÉ Gaillimh

# How to enforce strong Passwords?

- Minimum length (>8 characters)
- Capital and small letters mixed
- Letters, digits, and other symbols mixed
- Don’t reuse old passwords
- **Is all the above sufficient to create strong passwords?**

# Example for new Password Validation



Reset signin password

✓ Verify --- ✓ Enter New Password --- ✓ Done

New signin password

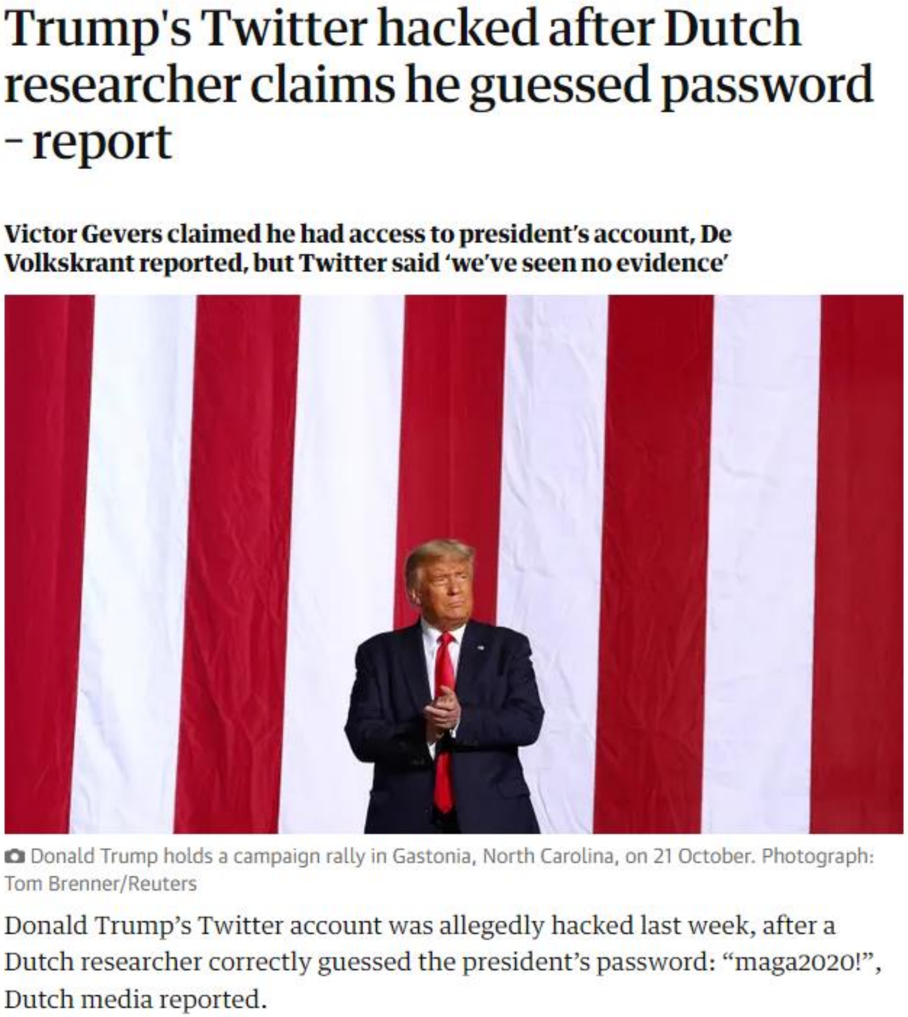
●●●●●●●●●●●

Middle

Confirm password

●●●●●●●●●●●

# The Guardian Headline



## Trump's Twitter hacked after Dutch researcher claims he guessed password – report

**Victor Gevers claimed he had access to president's account, De Volkskrant reported, but Twitter said 'we've seen no evidence'**

Donald Trump holds a campaign rally in Gastonia, North Carolina, on 21 October. Photograph: Tom Brenner/Reuters

Donald Trump's Twitter account was allegedly hacked last week, after a Dutch researcher correctly guessed the president's password: "maga2020!", Dutch media reported.

NUI Galway
OÉ Gaillimh

# maga2020! Who would use this Password?

- While this story is disputed by the US government, it shows the pitfalls of using readily available information for personal passwords
- BTW after the news broke, the apparent victim switched to two-factor authentication to access their Twitter account ;-)
  - Of course only until the person got banned from using Twitter :-)
- https://www.theguardian.com/us-news/2020/oct/22/trump-twitter-hacked-dutch-researcher-password

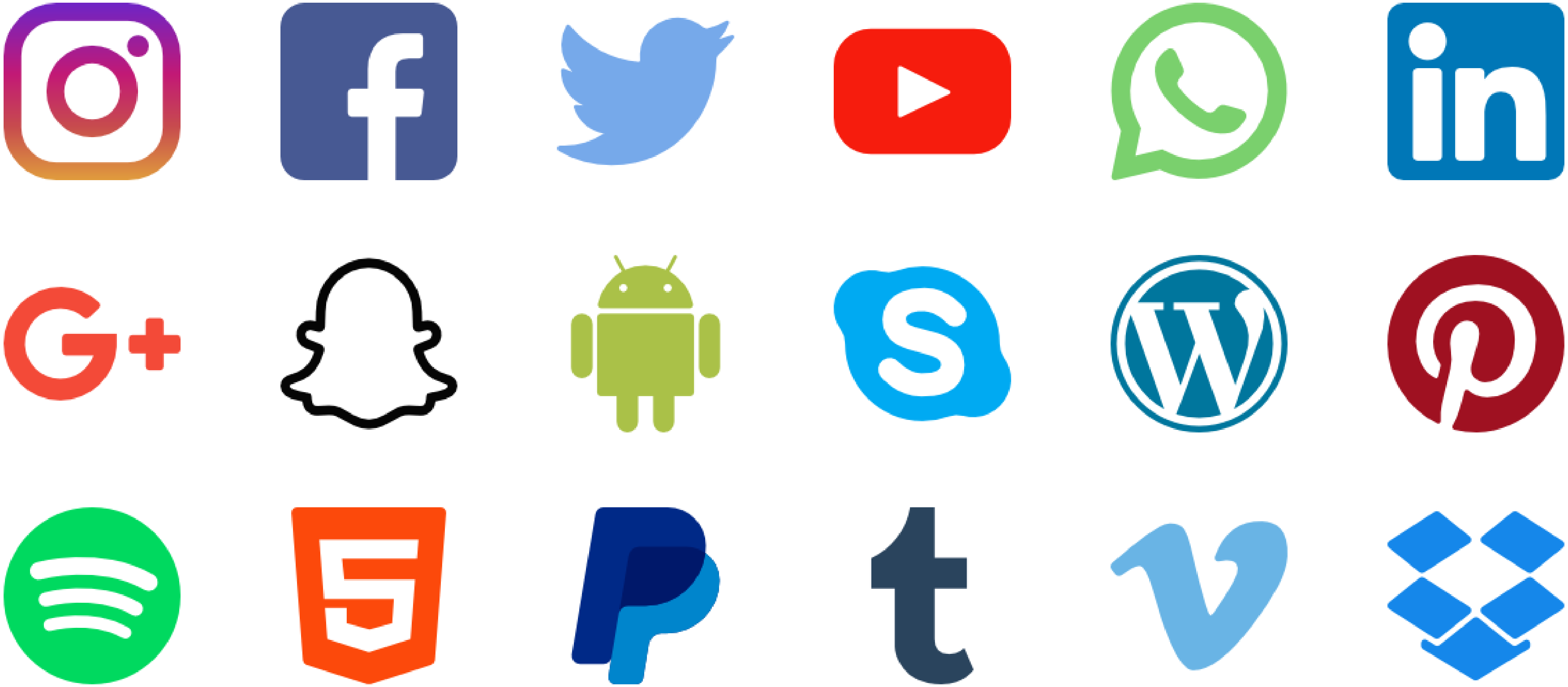
# The Human Factor

- In 2013 a Google research project concluded that
  - most people of use “readily available” information to generate passwords
  - subsequently some educated guesses often allow to reveal them
- So what is readily available information?

# Readily available Information

1. Pet names
2. A notable date, such as a wedding anniversary
3. A family member’s birthday
4. Your child’s name
5. Another family member’s name
6. Your birthplace
7. A favourite holiday
8. Something related to your favourite sports team
9. The name of a significant other

# Public Sources to retrieve such Information



# In-Class Activity: Your Personal Password Score

- Consider:
  - all **unique** passwords you currently use
  - your personal social media footprint; analyse your own posts for any “readily available” information that you incorporated into one of your current passwords
- Consider
  - direct and indirect information
  - password fragments

# In-Class Activity: Your Personal Password Score

- Direct information
  - E.g. your dog's name, e.g. password "Carly"
- Indirect information
  - E.g. a member of your favourite soccer team, for example password "Klopp" if you are a Liverpool FC fan
  - In your social media posts consider both text and images
- Password fragments
  - E.g. "!**Klopp**4ever" would qualify

# In-Class Activity: Your Personal Password Score

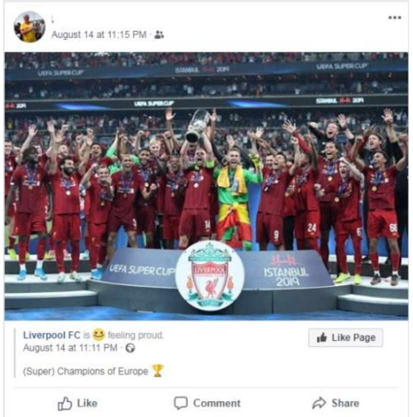
1. Estimate the total number of your passwords or password fragments that can be recovered via
   - direct information
   - indirect information

   retrieved from your social media footprint

   Note that each password should only count once, i.e. it can be either recovered or not
2. Divide both numbers by the total number of unique passwords that you use at the moment, and multiply the values with 100 (to get a percentage)

# Example

- Scanning my social media posts revealed that:
  - 2 password can be (fully or partially) revealed via direct information, as they contain the names of my pet rabbits mentioned in some of my posts: Leo and Enda
  - 4 password can be (fully or partially) revealed via indirect information (see Facebook post), i.e. they contain  (former) LFC players Alisson, van Dijk, Gomez and Firmino
- I use a total of 10 different passwords at the moment, therefore
  - (2/10) * 100 = 20%
  - (4/10) * 100 = 40%



August 14 at 11:15 PM

Liverpool FC is feeling proud.
August 14 at 11:11 PM

(Super) Champions of Europe 🏆

- In summary
  - 20% of my passwords are linked to direct information
  - 40% of my passwords are linked to indirect information
  - **Therefore, my personal password score is 60%, i.e.  More than half my passwords are linked to publically available information**

# In-Class Activity: Your Personal Password Score

- Please calculate / estimate your **personal password score** (0% - 100%)

# Scary Statistics about the Password Reuse Problem*

- A Google survey found that at least 65% of people reuse passwords across multiple sites
- Another recent survey found that 91% of respondents claim to understand the risks of reusing passwords across multiple accounts, but 59% admitted to doing it anyway
- The average person reuses each password as many as 14 times
- 72% of individuals reuse passwords in their personal life

*Source: https://securityboulevard.com/2020/04/8-scary-statistics-about-the-password-reuse-problem/