cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

UNIVERSITY OF Southampton

COMP6224
User Authentication – Passwords

Dr Federico Lombardi

f.lombardi@soton.ac.uk

Cybersecurity Southampton

CyberSecuritySoton.org [w]

@CybSecSoton [fb & tw]

This week

- User Authentication
  - Password-based
  - Token-based
  - Biometric

Lecture Outline

- User based authentication
  - Password Based Authentication
  - Password Attacks
  - Possible Countermeasures

Learning outcomes

At the end of this session, you should be able to:

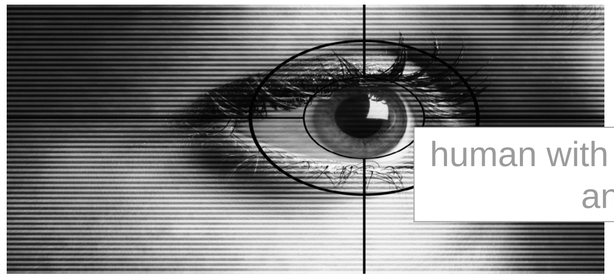
- Understand different existing approaches to authenticate users
- Define different types of attacks to password authentication and their countermeasures
- Describe the use of token-based and biometric user's authentication, and their limitations

User Authentication

- Fundamental security building block
- It is the process of verifying an identity claimed by a system entity
- Consists of two steps:
  - **Identification**: present an identifier to the authentication system
  - **Verification:** verify the validity of the presented identifier

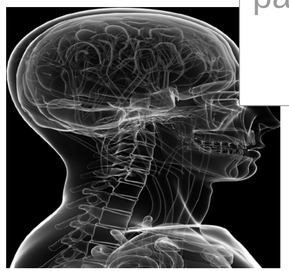
User Authentication

- Three possible approaches
  - something the person **knows** (like a password),
  - something the person **has** (like a smart card or a radio key fob storing secret keys),
  - something the person **is** (like a human with a fingerprint)



human with fingers and eyes

Something you are



password=uclb()w1V
mother=Jones
pet=Caesar

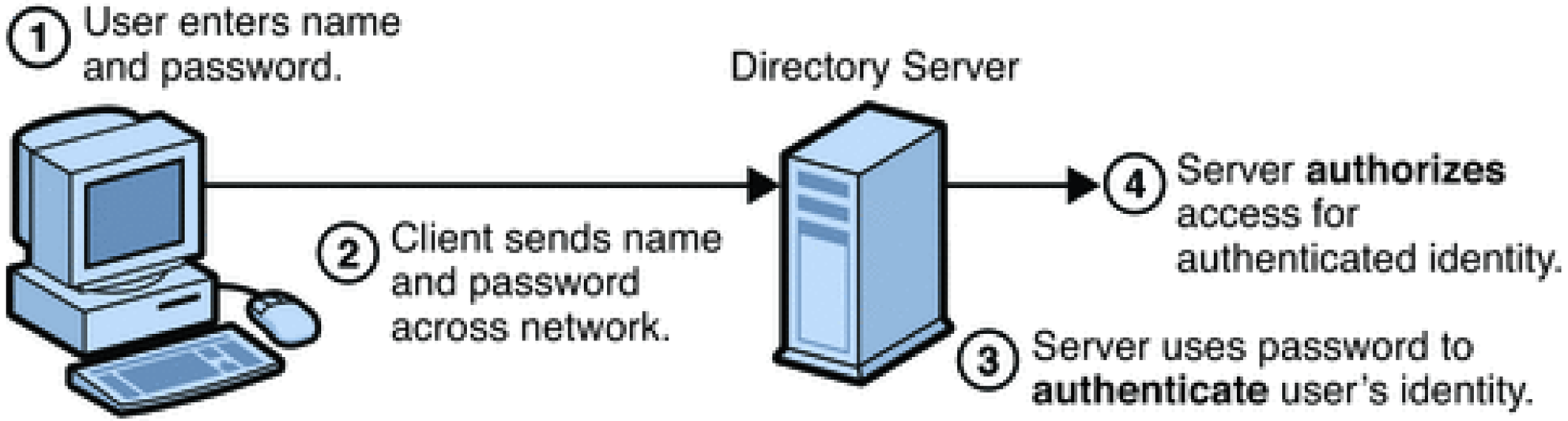
Something you know

radio token with secret keys

Something you have

Password Authentication

- Password authentication and authorisation



Similar Concept or same thing?

Authentication vs Authorisation… differences?

Similar Concept or same thing?

Authentication vs Authorisation… differences?

Authentication

Who you are

Authorization

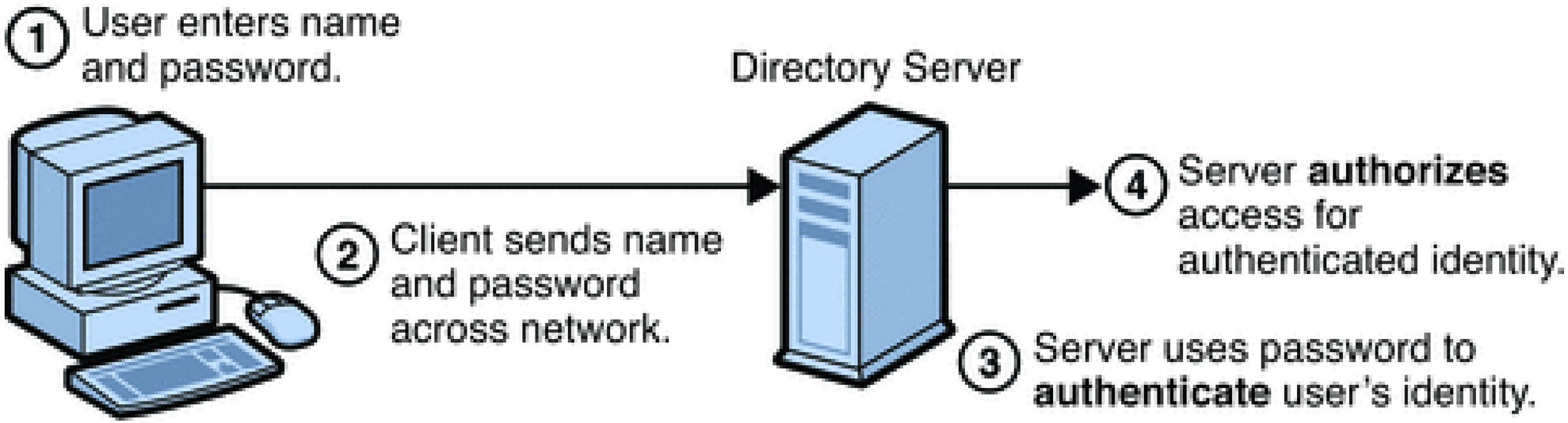
What you can do

Who has to be authenticated?

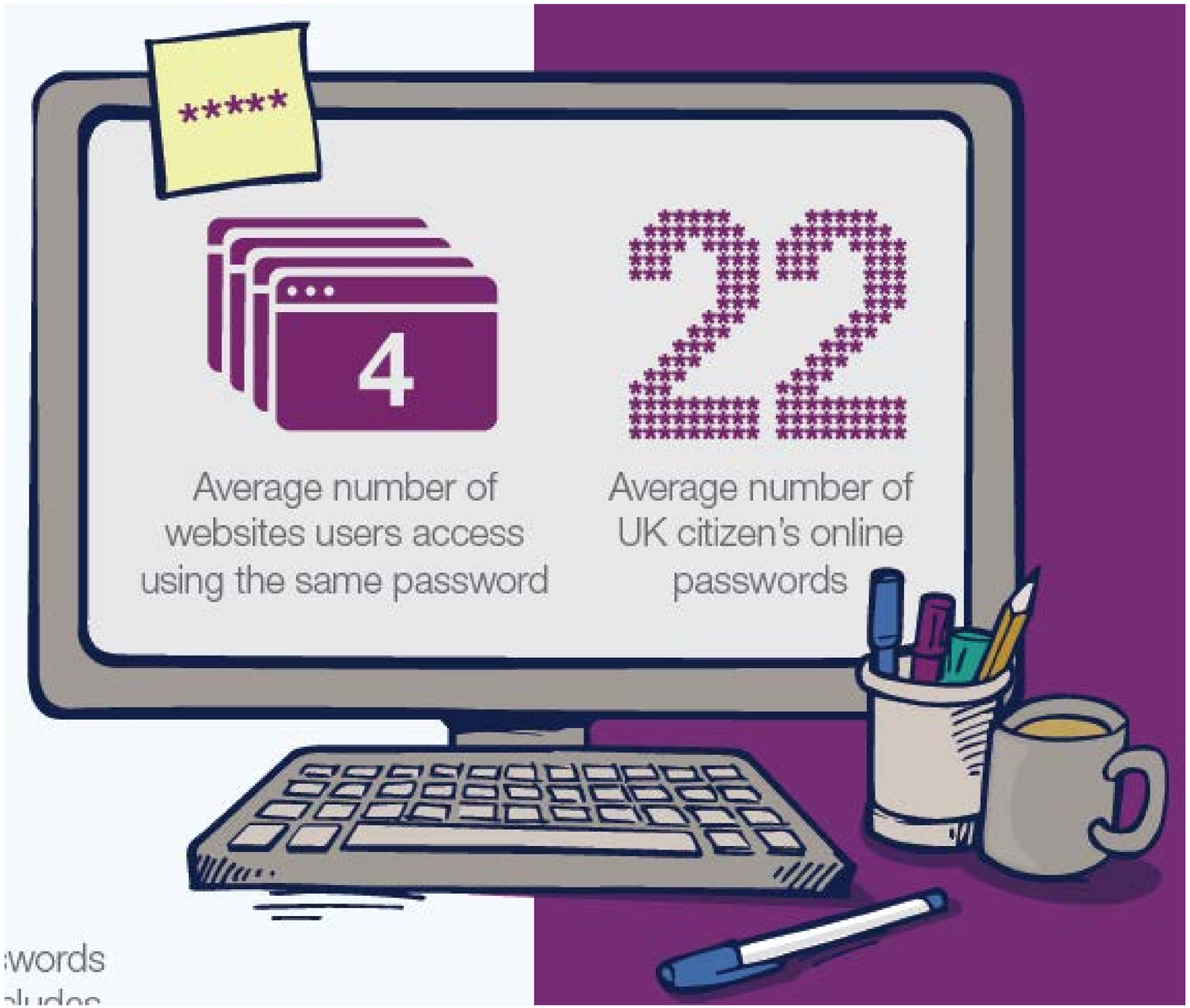
- Client authentication
- Server authentication

Password Authentication

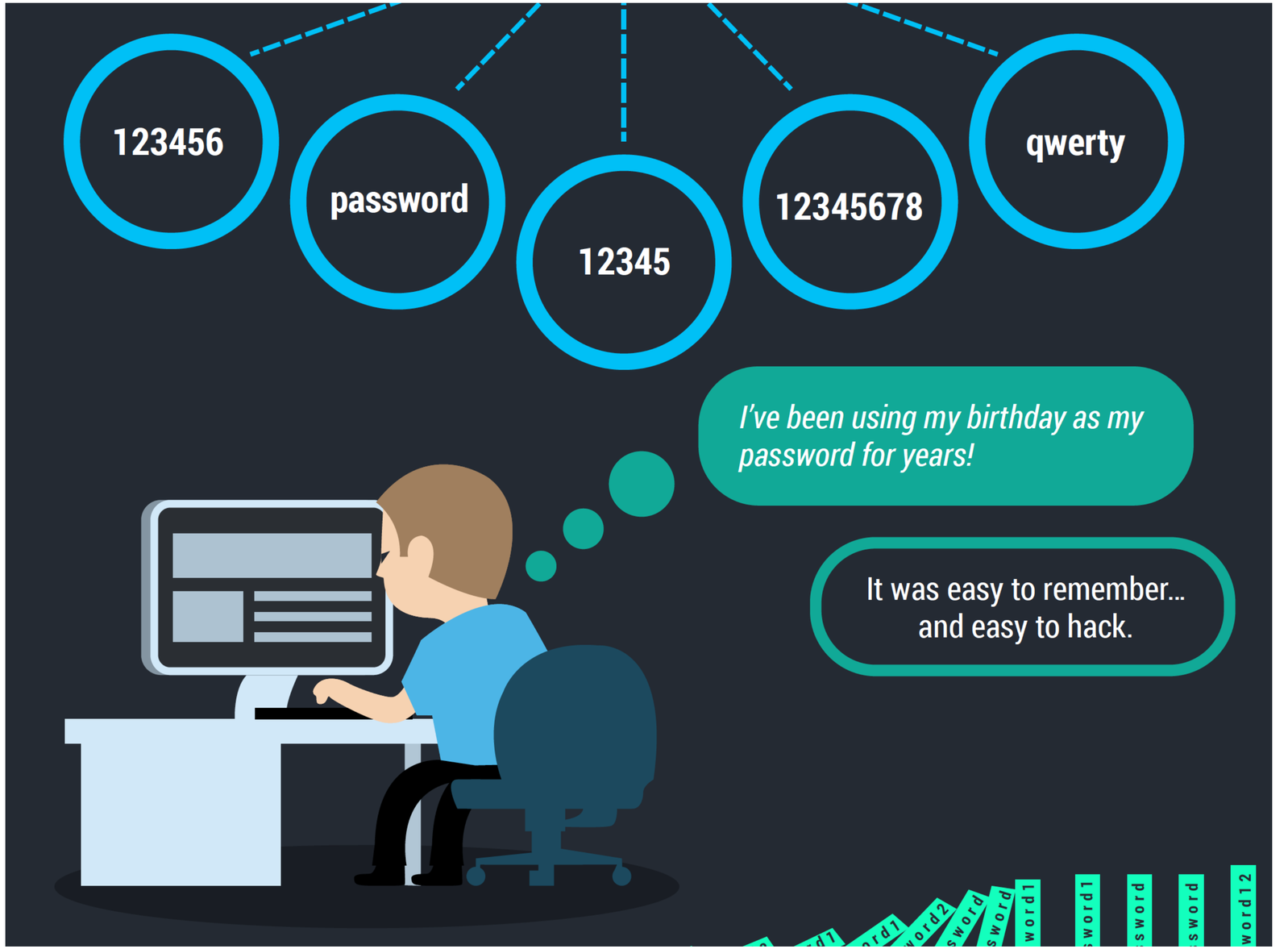
- widely used user authentication method
  - user provides username and password
  - system compares password with that in the password file
- authenticates ID of user logging and
  - that the user is authorized to access system
  - audit logs



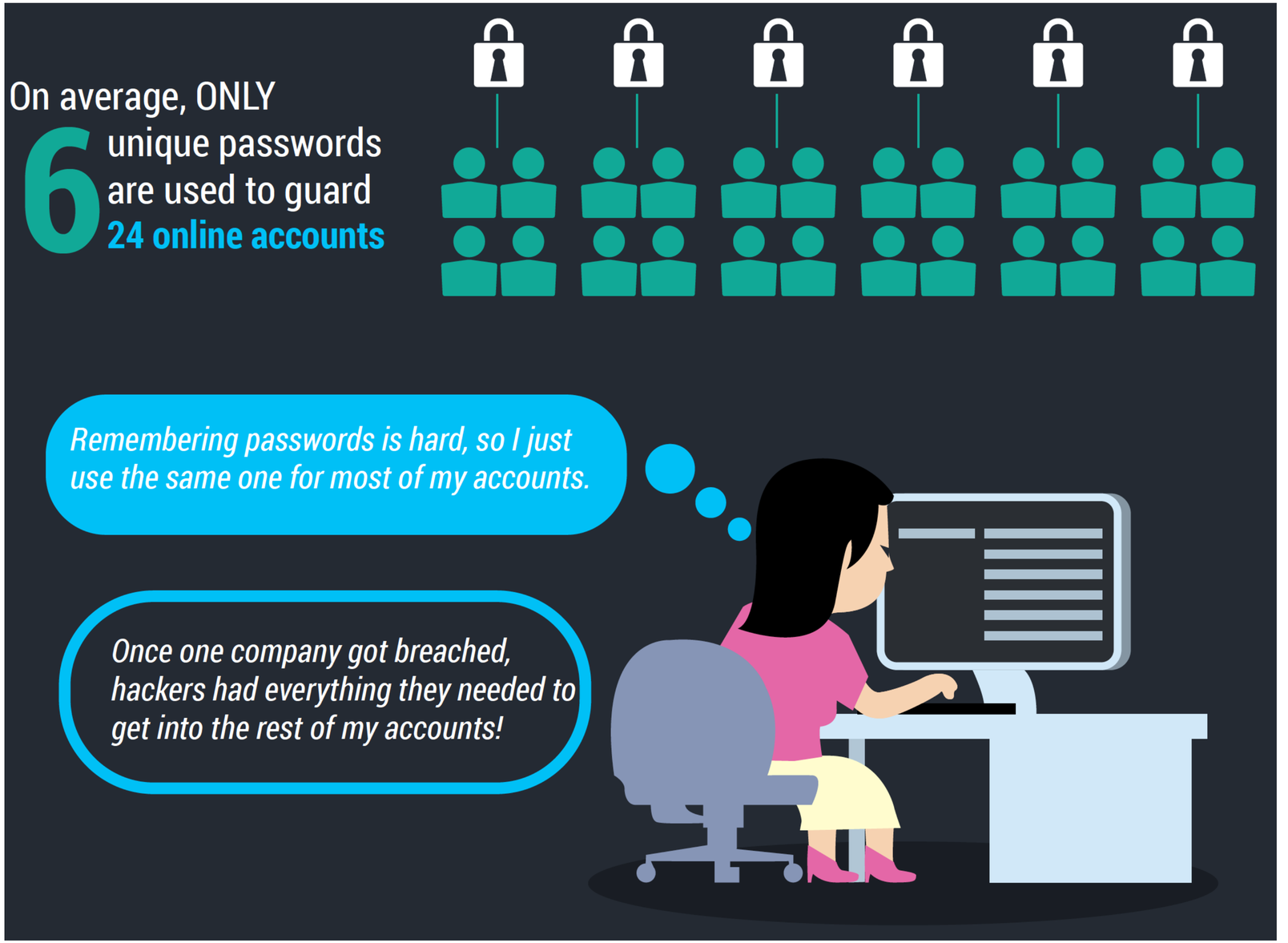
Password Overload problem



Predictable passwords



Password Reuse



UNIVERSITY OF Southampton

In the past year, 2 in 5 people:

Received a notice that their personal information had been compromised

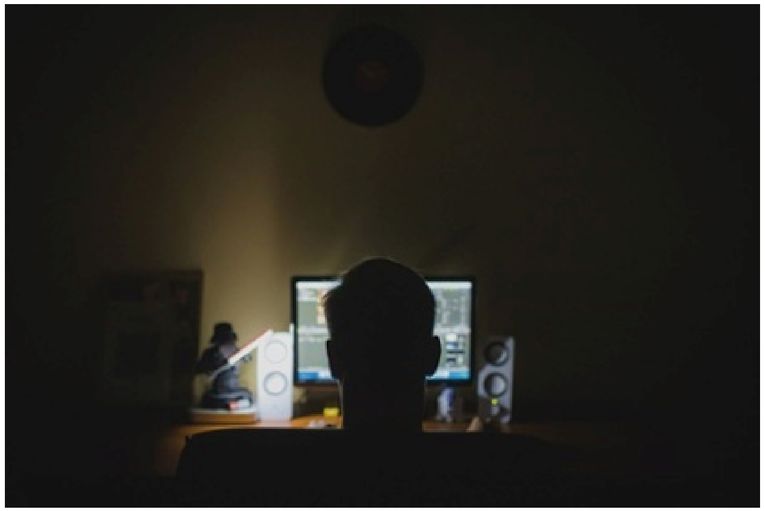
Had an account hacked

Had a password stolen

63% of Data Breaches Result From Weak or Stolen Passwords

In its recent **2016 Data Breach Investigations Report**, Verizon Enterprise confirmed many industry trends that we see at ID Agent every day. The most glaring blind spot for organizations is how stolen credentials are the primary means by which hackers exploit their vital systems.

Credentials are the holy grail for hackers. In a study of 905 phishing attacks, the vast majority—91 percent—were after user credentials.

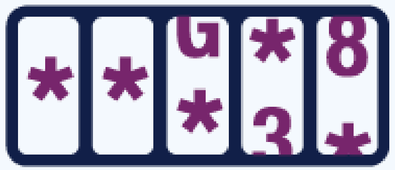


Stolen Credentials Are a Big Problem That You May Not Know About

iCloud Attack

- August 2014 the Apple's iCloud account were hacked
- a collection of almost 500 private pictures of various celebrities, mostly women were posted on image boards like 4 chan and other social media
- victims' iCloud account information was obtained using phishing and brute force guessing
- Attacker indicated that one user created a fake email account called **appleprivacysecurity** to ask celebrities for security information

How passwords are cracked?



Brute Force

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

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Interception

Passwords can be intercepted as they are transmitted over a network.

Shoulder Surfing

Observing someone typing their password.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Searching

IT infrastructure can be searched for electronically stored password information.

Key Logging

An installed keylogger intercepts passwords as they are typed.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Brute Force Attacks

- Exhaustive search
  - Try all possible combinations of symbols up to a certain length
  - The size of the password space is $|A|^n$

- Assume a 8 characters password
  - Upper- and lowercase letters, digits, common symbols (96 possible characters)
  - 96^8 = 7.2 quadrillion password combinations

How long does it take to crack a password?

Password strenght

- **Password strength** measures the effectiveness of a password against **brute force** attack

- It estimates the number of trials an attacker has to make to guess the password correctly

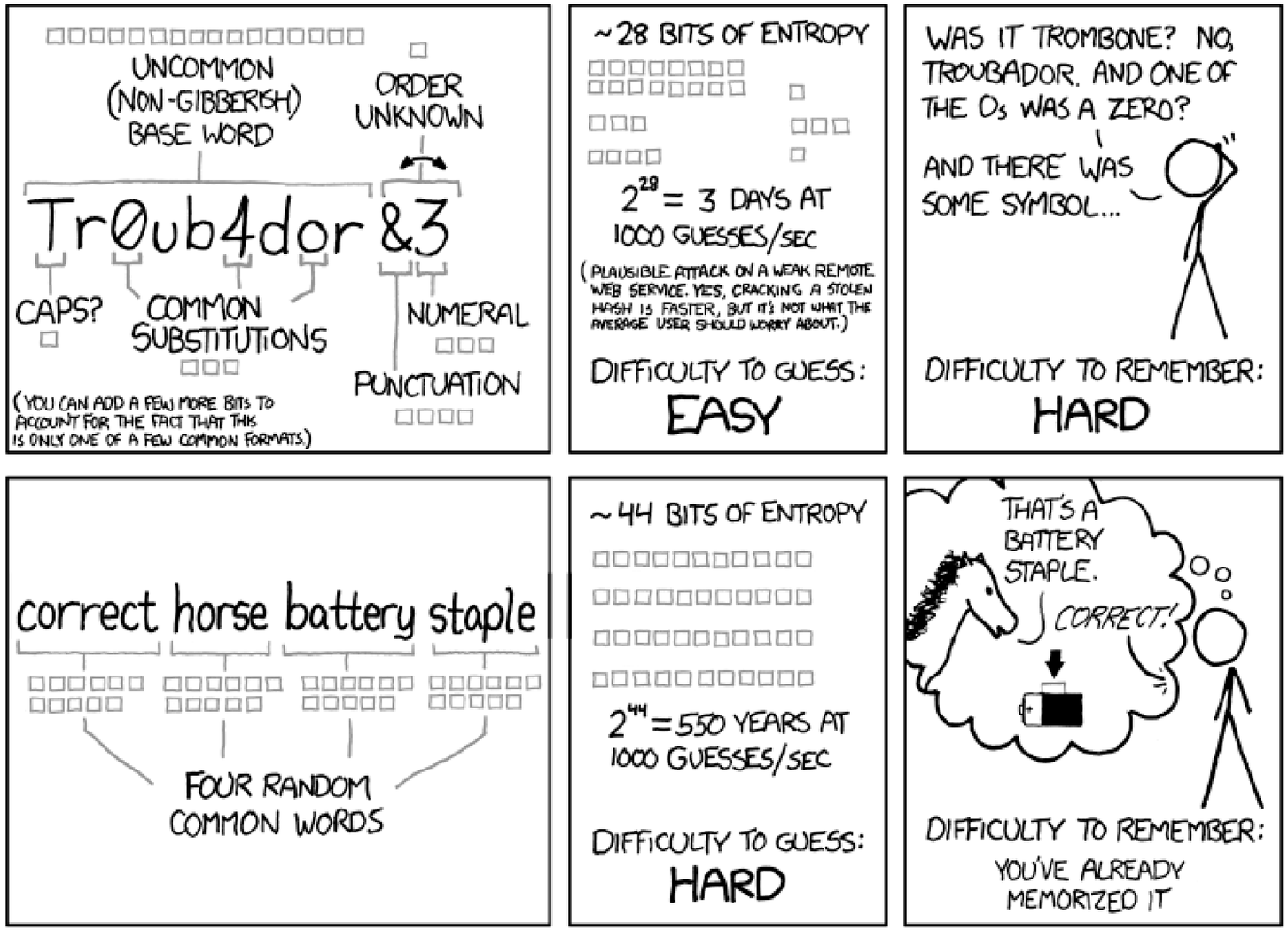
- It is normally computed as $|A|^n$
  - ***A*** is the set of symbols composing the password
  - ***N*** is the length of the password

Password strenght

- **Password strength** measures the effectiveness of a password against **brute force** attack
  - ***A*** is the set of symbols composing the password
  - ***N*** is the length of the password

- Another measure is **entropy**
  - $\mathbf{Log_2}\,|A|^n = n\,\mathbf{Log_2}\,|A| = n\,\mathbf{Log}\,|A|/\text{Log } 2$
  - It is typically measured in bits
  - If the entropy of a password is **b** bits it means the attacker requires to $\mathbf{2^b}$ attempts

Password strength



zxcvbn

	qwER43@!	Tr0ub4dour&3	correcthorsebatterystaple
zxcvbn	Weak	So-so	Great!
Dropbox (old)	Great!	Great!	So-so
Citibank	Medium	Strong	1 number required

- Match a password against all the possible patterns
  - Dictionaries of common words
  - Keyboard patterns
  - Repeated letters e.g rrrrr
  - Years from 1900 to 2019
  - Dates
- Calculates an entropy for each matched pattern
  - Entropy (rrrrr) = lg(26*5) about 7 bits of entropy
- Password’s entropy is the same of the entropy of constituent patterns
  - entropy(“stockwell4$er123698745) = entropy (“stockwell”)+entropy(“4$eR) +entropy (“123698745”)

Entropy means security?

UNIVERSITY OF Southampton

Entropy means security?

Yes and no!

Mathematically yes, but it does not consider dictionary

That explains why …

zxcvbn

	qwER43@!	Tr0ub4dour&3	correcthorsebatterystaple
zxcvbn	Weak	So-so	Great!
Dropbox (old)	Great!	Great!	So-so
Citibank	Medium	Strong	1 number required