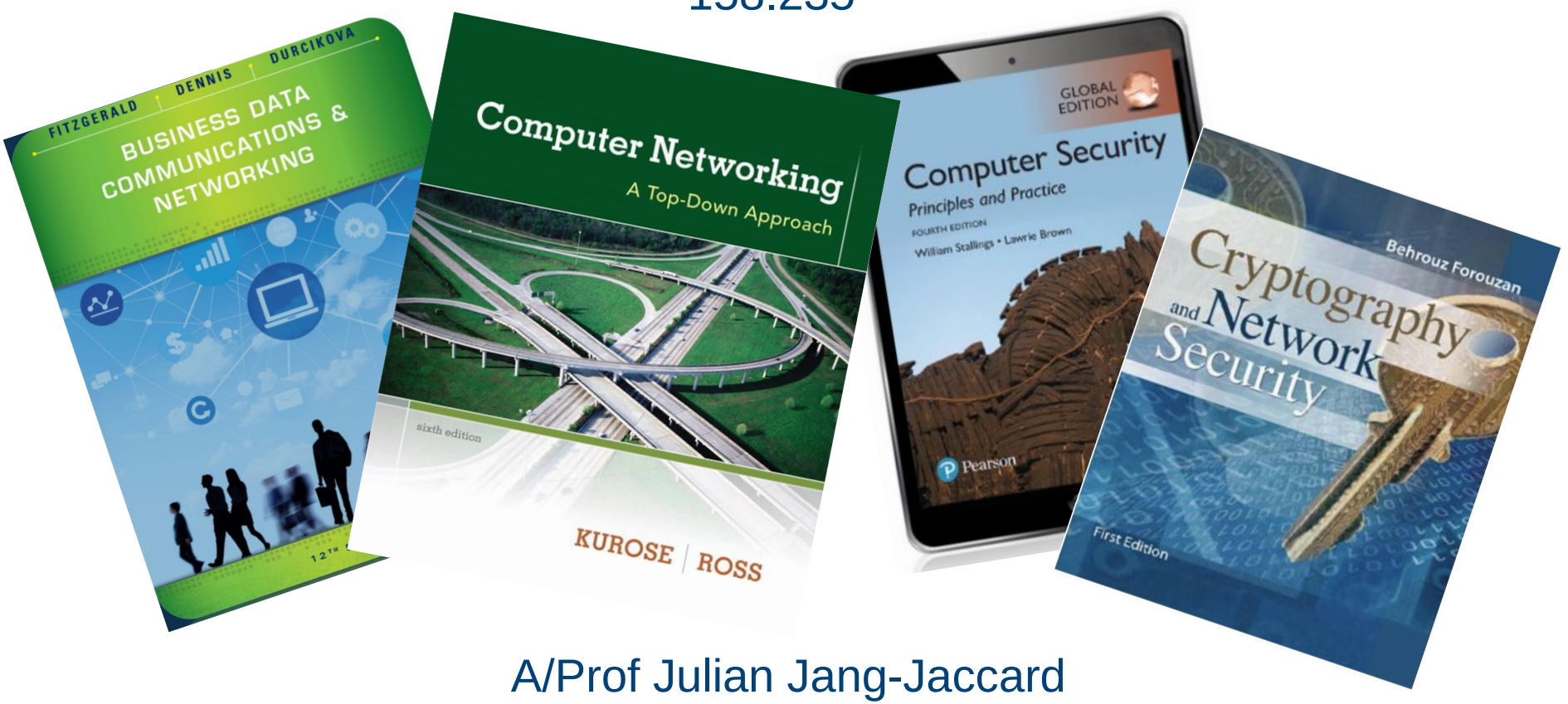
MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Network, Security and Privacy

158.235



A/Prof Julian Jang-Jaccard

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Authentication

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Essential Terms

- Identification= process by which system entity provides a claimed identity to the system, *for example a user ID like alice or bob or 93123.*
- Authentication= process of verifying an identity claimed by or for a system entity, *for example using a password.*
- Authorisation= granting of a right or permission to a user or system entity to access a given resource.
- *System entity*= user, program, device ...

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Authentication

- Three means of authenticating (or called user factors) user identity are based on:
  - Something you know
  - Something you have
  - Something you are

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Something you know

- Users gain access based on something they know
- Password based
  - Must kept secret
  - Easy to recall
  - Unique
  - Should be long and complex
- Password Weaknesses
  - Not very secure due to poor choice of passwords
  - Because human beings can memories only a limited number of items
  - Produce weak passwords
  - Security policy enforcement doesn't help

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

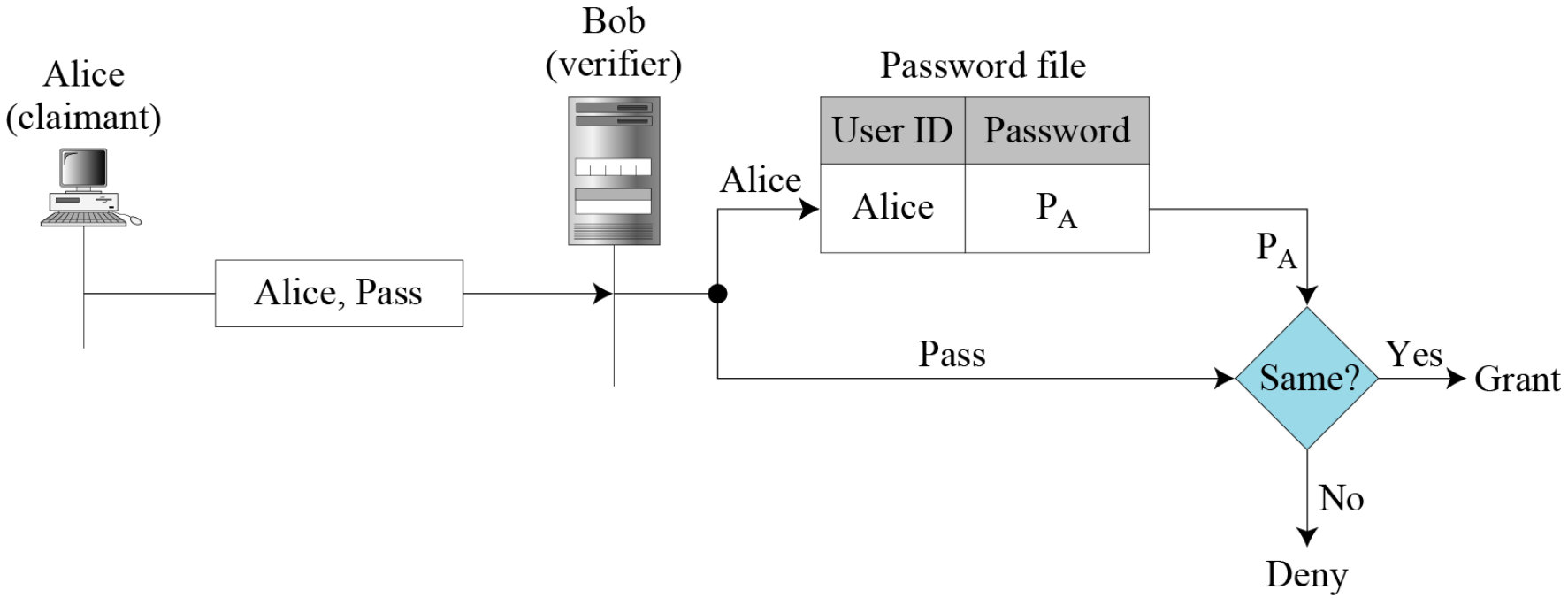
Examples: 10 most used passwords

Passwords: First Approach

User ID and password file

P_A: Alice's stored password

Pass: Password sent by claimant

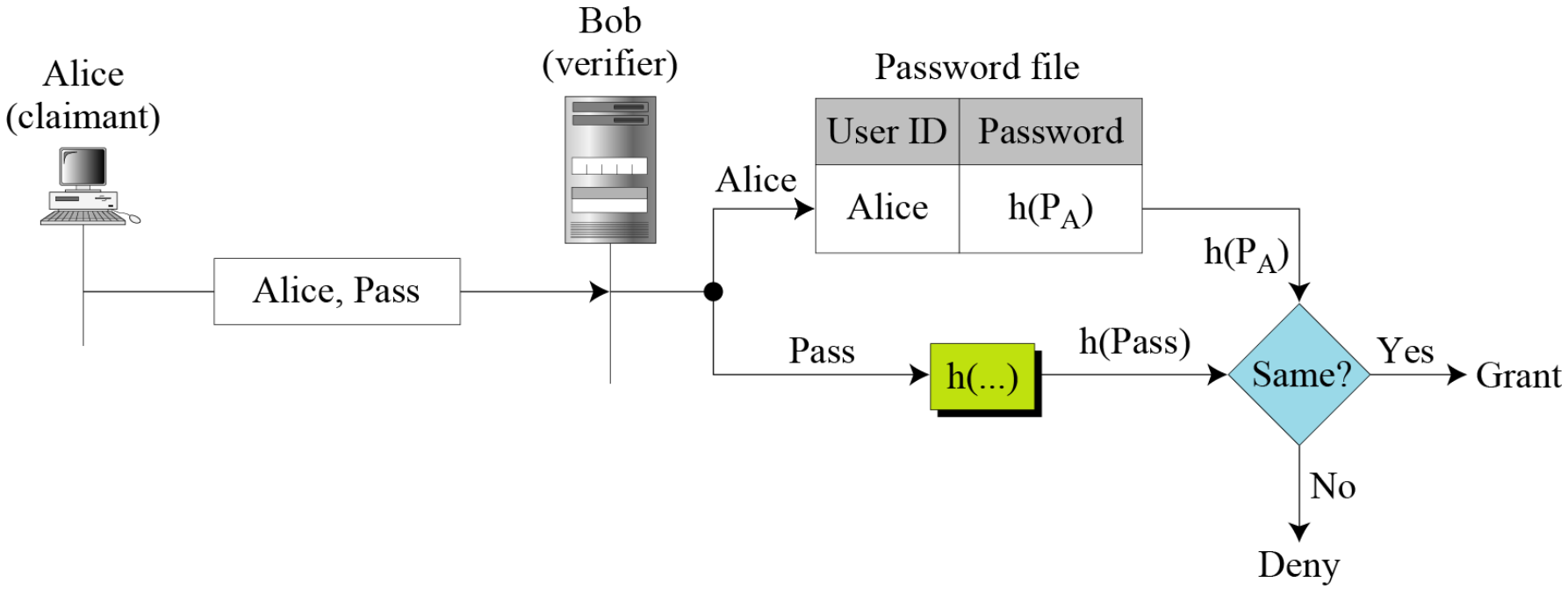


Passwords: Second Approach

Hashing the password

P_A: Alice's stored password

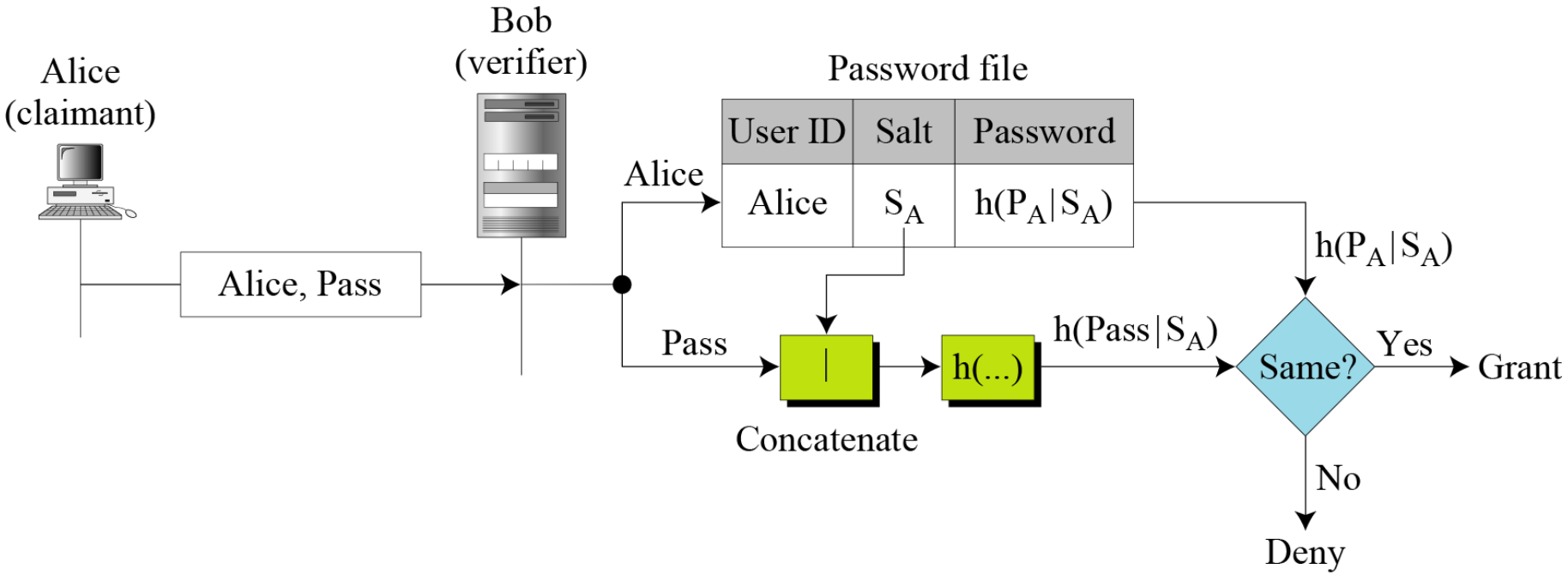
Pass: Password sent by claimant



Passwords: Third Approach

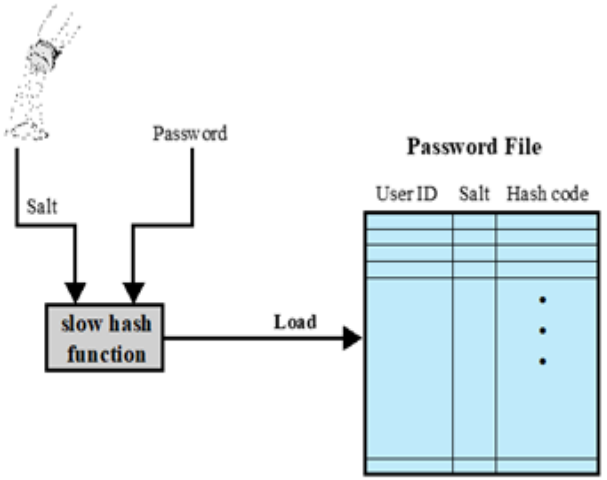
Salting the password

P_A: Alice's password
S_A: Alice's salt
Pass: Password sent by claimant



Salting and Hash: Loading Password

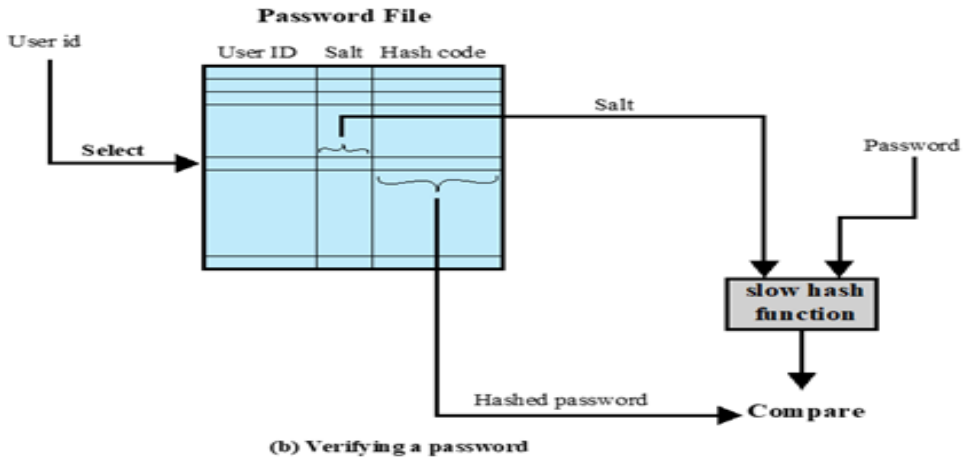
- Salt : idea is to increase attacker workload by increasing the complexity of the hash
- Salt = pseudorandom or random number
- User supplies password
- Hash applied to combination of salt & password
- Store userID salt and hash in the password file (or database)
- Password is not stored!
- Password files often hidden (shadow passwords in Unix, only accessible to system admin)



(a) Loading a new password

Salting and Hash: Verifying Password

- User provides their ID and password.
- Lookup the salt and hash.
- Recompute the hash using the supplied password plus salt.
- Does the recomputed hash equal to what was expected?
- Note that this scheme never reveals the password to anyone, even to system admin



MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Password Cracking

- Brute force Attack
  - Attempt on every possible combination of letters, numbers, and characters
  - Create candidate digests (called rainbow table) for matching
  - Computation intense
- Dictionary Attack
  - Begins with creating digests of common dictionary words or their mutations
    - e.g. p@ssw0rd, Luv4Eva
  - Intelligent cracker tool will apply those mutations automatically
  - Password dictionaries, contain paswords that are either very popular or were captured during previous attacks) also can be used.

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

2 Factor Authentication (2FA)

- Two factor because “what you know” (password) + “what you have” (device)
  - –Enter password, sent text message with special code and must enter this to complete verification
  - –Can also be a token (SecureID etc.) that automatically generates special code
  - –Or an app on your phone (Google authenticator)
- Special code is a one time password
  - –Never used twice.
  - –Randomly generated.
- Generalised to multifactor authentication (MFA).

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Something you have

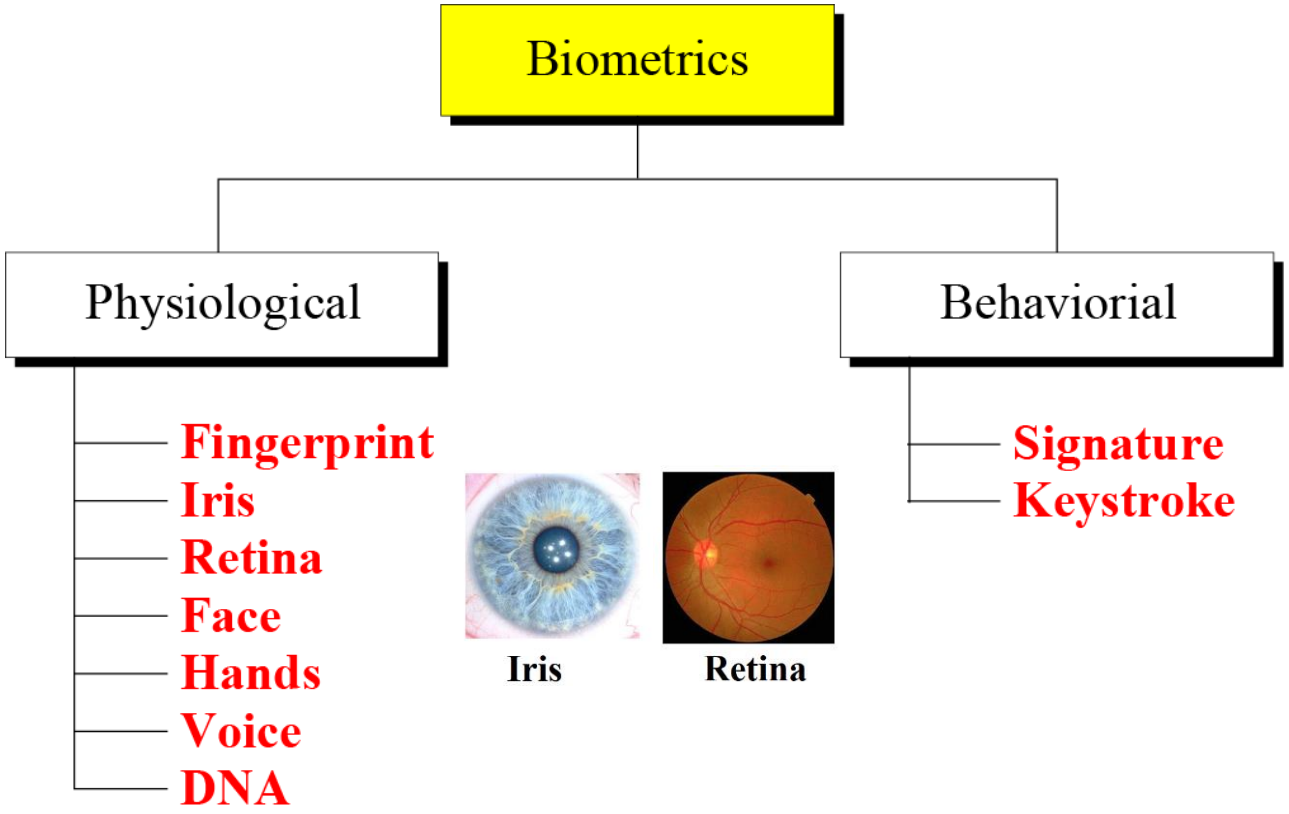
- Users gain access based on presenting something they have
- Something human owns that can authenticate the holder
  - For example, Security Card, Security (hardware) tokens

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Something you are (Biometrics)

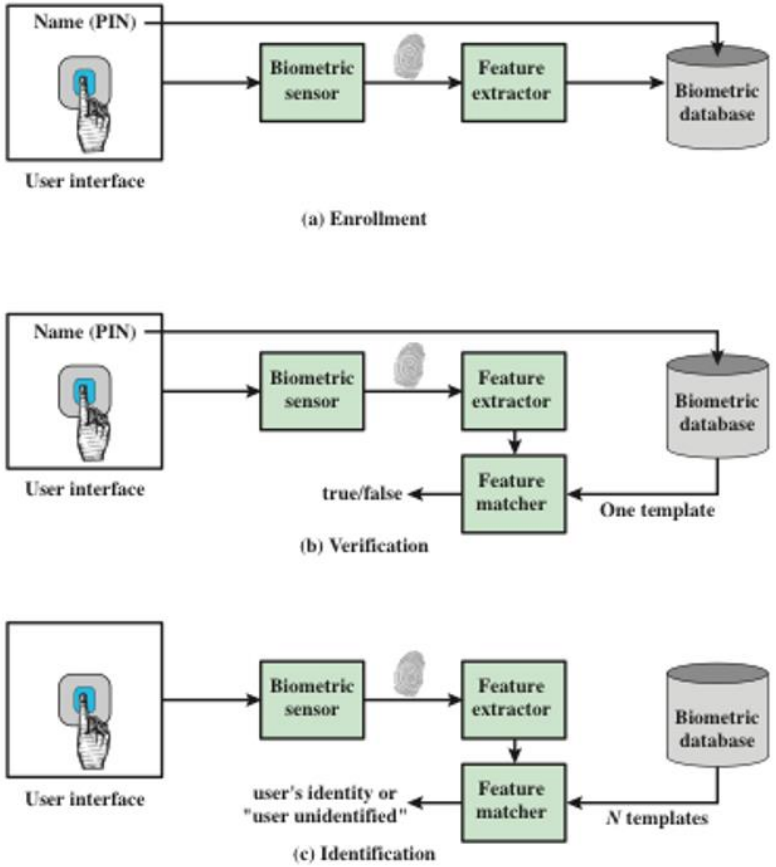
- Users gain access based on something they are (either Physiological or behavioral features)
- Based on pattern recognition
- Is technically complex and expensive when compared to passwords and tokens
- Becoming more common due to fingerprint readers etc. being built into mobile phones.

Biometrics

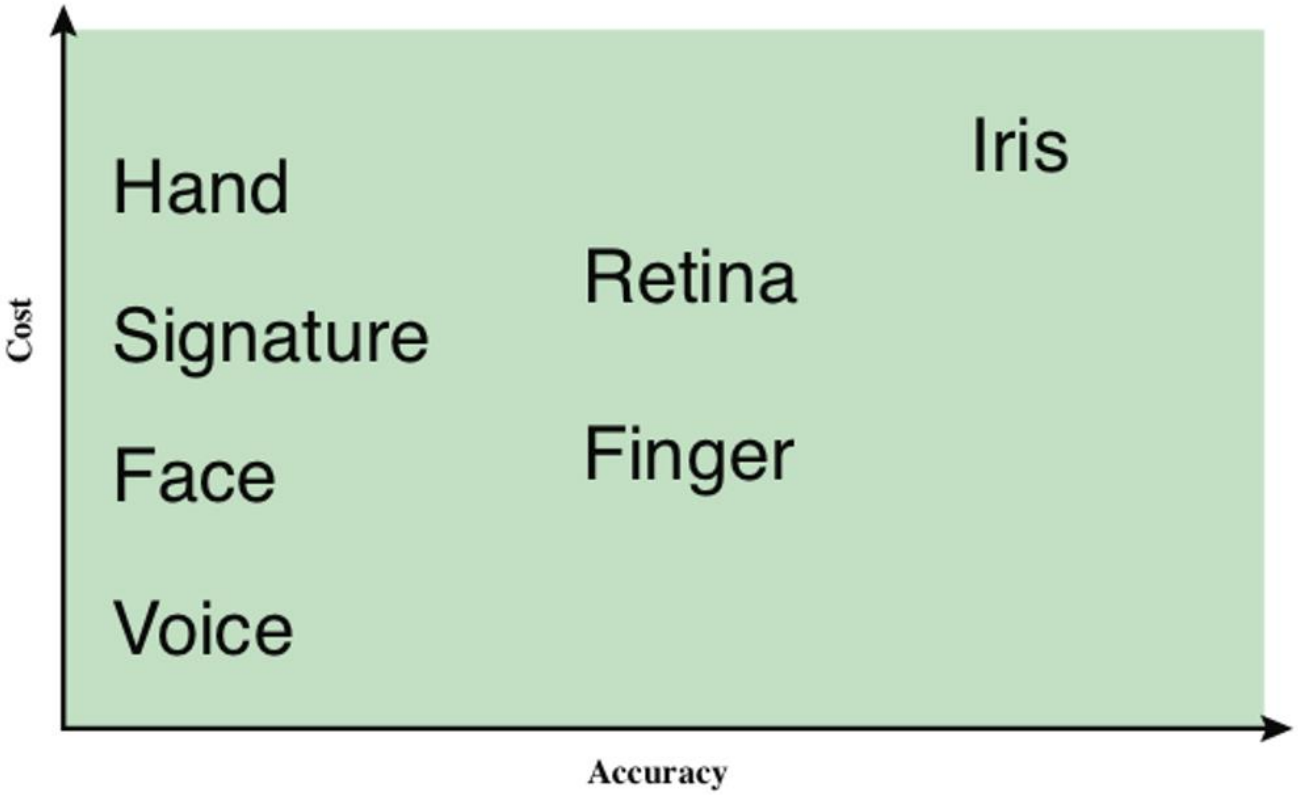

Biometrics
Physiological
Behaviorial
Fingerprint
Iris
Retina
Face
Hands
Voice
DNA
Signature
Keystroke
Iris
Retina

Biometrics: how it works

- Pattern recognition.
- Face: relative location and shape of key facial features.
- Fingerprint: furrows and ridges.
- Hand geometry: shape, lengths and widths of fingers.
- Retinal pattern: veins illuminated by low-intensity beam of light.
- Signature: writing habit, pressure, shape of signature, will vary over time (dynamic).
- Voice: based on anatomy and physical characteristics, will vary over time as well (dynamic).
- *NOT 100% ACCURATE UNLIKE A PASSWORD*



Biometrics


Hand
Signature
Face
Voice
Retina
Finger
Iris
Cost
Accuracy

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

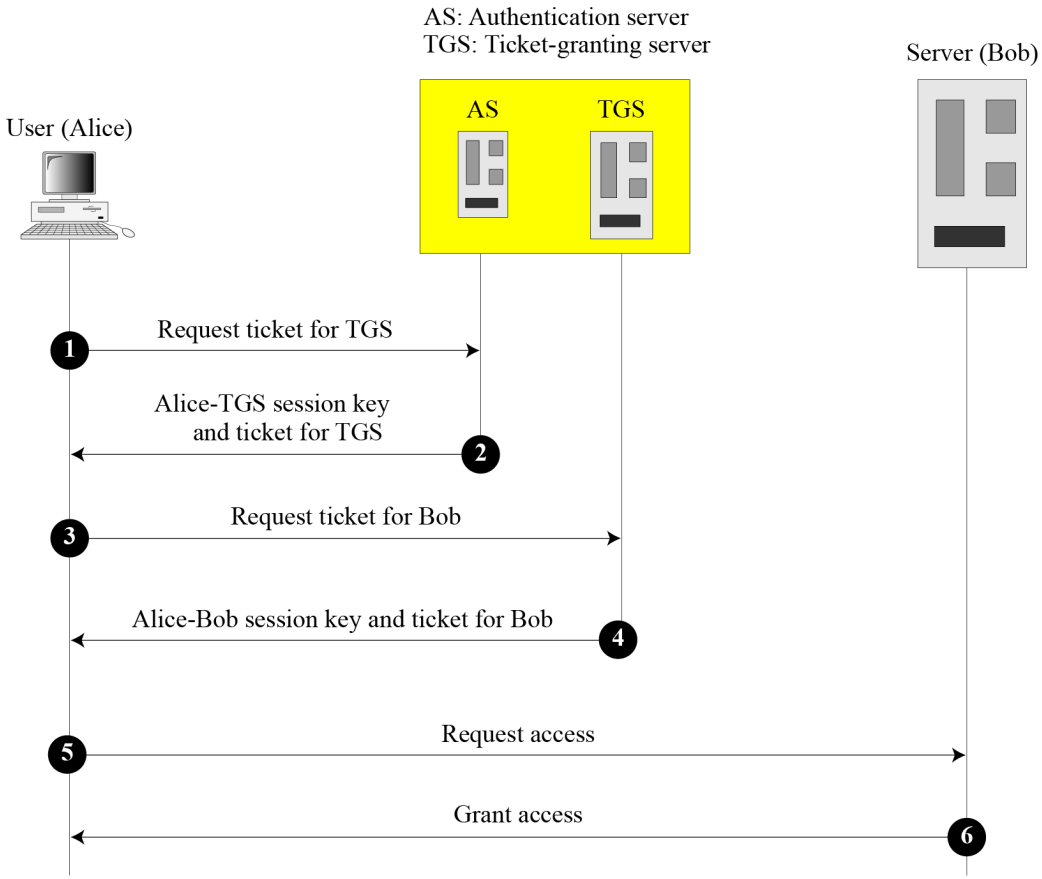
Central Authentication

- Also called Single Sign-On (SSO)
  - Allows users to access multiple services with a single login
  - Provides a single access to multiple systems within a single organisation
- Phase 1: Requires user to login to an authentication server
  - Checks id and password against a database, then a certificate
- Phase 2: Certificate used for all transactions requiring authentications
  - No need to re-enter passwords, Eliminates passwords changing hands

Kerberos

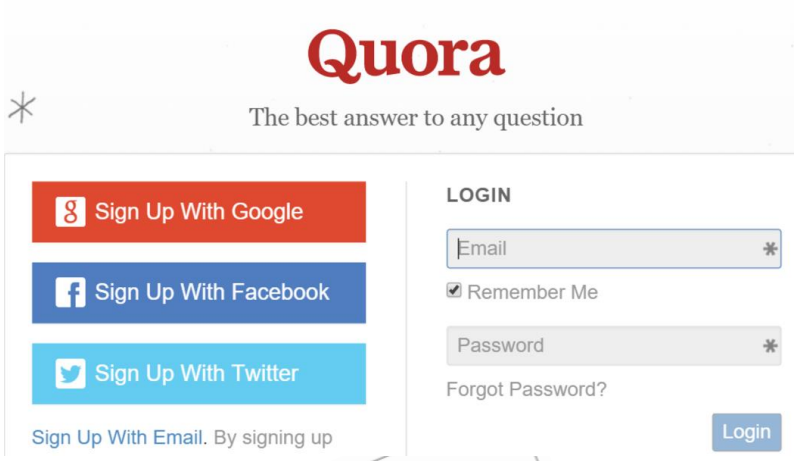
- Is an authentication server that acts as a third-party authenticator
  - Helps the user to prove its identity to the various services
- The three heads
  - Authentication
    - Confirms that a user who is requesting services (user certificate)
  - Authorization
    - Granting of specific types of service to a user based on their authentication (ticket)
  - Accounting
    - Logs the ticketing of the consumption of network resources by users

Kerberos


AS: Authentication server
TGS: Ticket-granting server
Server (Bob)
AS
TGS
User (Alice)
1
Request ticket for TGS
Alice-TGS session key
and ticket for TGS
2
3
Request ticket for Bob
Alice-Bob session key and ticket for Bob
4
5
Request access
Grant access
6

OAuth Shift

- Moving enterprise authentication server to the Web
- Called as HTTP-based Single Sign-On
  - Similar in spirits with Kerberos, OpenID, SAML
- Strictly speaking, it's a Federated Identity
  - Provides a single access to multiple systems across multiple organisations
- Open Standard allows Internet users to log in to 3rd party websites
  - Sign their accounts at Google, Facebook etc.,



MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

OAuth Benefits

- Authentication and Authorization provided by third party Service Provider
  - Application developers can focus on building an app, not an authentication framework
- Username and password are not processed by application
  - User identification is collected by service provider
  - Improves Usability and security
- Centralized management of user accounts
  - Users don't need to create separate account for each application/service
  - Fewer identities & passwords to remember

OAuth Service Providers and Clients

- OAuth Service Providers:
  - For web access to Google APIs
    - Google+, Drive, AdSense, Analytics, and many more...

    Google
  - Web and Streaming (real time) APIs

    twitter
  - Using Graph API (ie a low-level HTTP-based API) to get data in and out of Facebook's platform

    facebook
- OAuth Clients
  - Websites:
    - CNN, Washington Post, Gawker, Kickstarter, La Crosse Tribune, etc.
  - Mobile apps & games
    - According to Facebook, 81 of the top 100 grossing iOS apps and 62 of the top 100 grossing Android apps use Login with Facebook
  - Anything with a "Log in with Facebook/ Google +/Twitter" option

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Social Engineering

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Social Engineering

- "Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology."

Kevin Mitnik et. al. from *The Art of Deception: Controlling the Human Element of Security (2002).*

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

People Hacking

- People are the weakest link in any security system.
- *"Only amateurs attack machines; professionals target people."* *Bruce Schneier*
- *Exploits people's trusting nature.*
- Hardest thing to defend against.

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Targets

- Effective social engineers can obtain the following information for examples;
  - User passwords
  - Security badges or keys to the building and even to the computer room
  - Intellectual property such as design specifications, source code, or other research and development documentation
  - Confidential financial reports
  - Private and confidential employee information
  - Personally-identifiable information (PII) such as health records and cardholder information
  - Customer lists and sales prospects

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Baiting

- Promise of item or good that is desirable to the victim.
- 20 USB sticks left in parking lot.
- Each contained an image and trojan horse malware.
- 16 out 20 plugged them into their computer.

Quid Pro Quo

- Benefit in exchange for information
- A study, 90% of office workers at Waterloo Station in the UK gave away their computer password for a cheap pen (men were worse than women by difference of 5%).
- Similar studies involving chocolate bars.

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Tailgating

- Can’t get into a building?
- No problem, just wait until someone with access enters the building and follow after them.
- Strike up conversations with employees(become a smoker) to increase trust.
- Also known as “piggy backing”.

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Other examples

- Typo Squatting: rely on typo goggle.com instead of google.com
- Hoaxes: false warning such as deadly virus
- Dumpster Diving: digging through trash receptacles
- Shoulder Surfing: observing victim's action

Spanish Prisoner Scam

- Confidence trick.
  - -Gain confidence (trust) of a mark
  - -Defraud them
- Spanish prisoner scam
  - -Wealthy prisoner
  - -False identity
  - -Small amount needed to release
  - -Monetary and non-monetary reward
  - -Unexpected expenses

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

How to

1. Define your goal.
2. Seek information about victim.
3. Build trust.
4. Exploit the relationship.
5. Use the information gathered for malicious purposes.

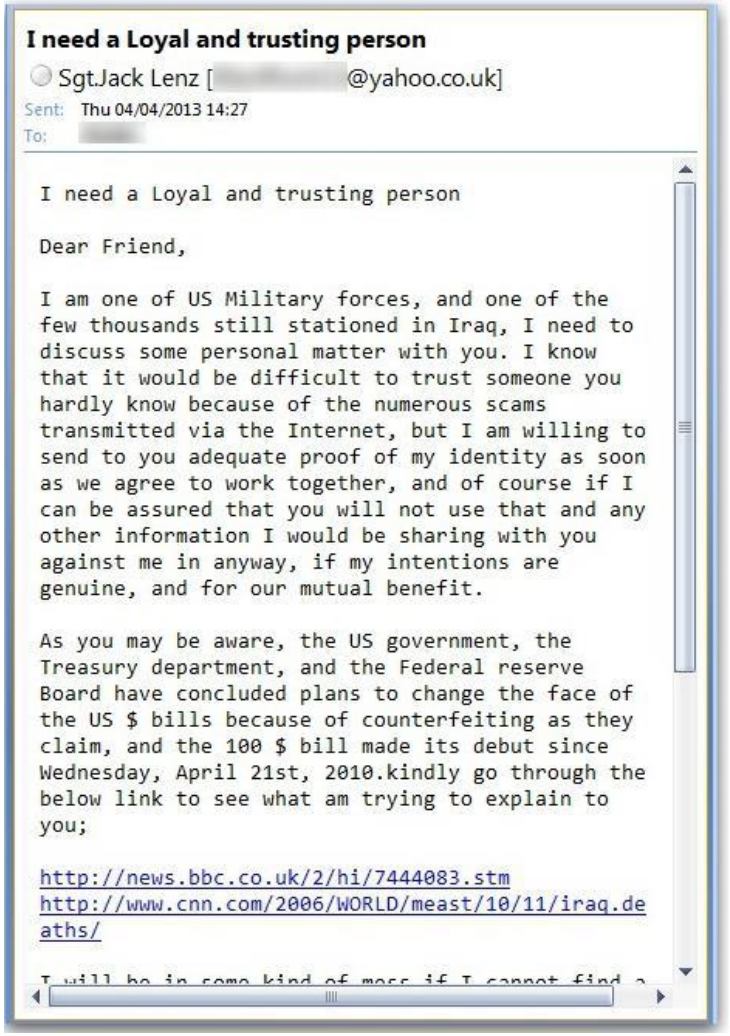
MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Role of Internet

- Previously one-to-one interaction, now one-to-many via email or social media platforms
- Larger number of marks means larger absolute number of marks who fall for the scam
- People find it hard to make trust judgements in the absence of body language and other signals that you get in a one-to-one interaction

419 Scam

- 419 is a number of a penal code in Nigeria (although most scammers are in the USA).
- Small outlay, get something of much greater value.
- Many variations of central idea:
  - -Romance
  - -Jobs
  - -Pets



I need a Loyal and trusting person

Sgt.Jack Lenz [@yahoo.co.uk]

Sent: Thu 04/04/2013 14:27

To:

I need a Loyal and trusting person

Dear Friend,

I am one of US Military forces, and one of the few thousands still stationed in Iraq, I need to discuss some personal matter with you. I know that it would be difficult to trust someone you hardly know because of the numerous scams transmitted via the Internet, but I am willing to send to you adequate proof of my identity as soon as we agree to work together, and of course if I can be assured that you will not use that and any other information I would be sharing with you against me in anyway, if my intentions are genuine, and for our mutual benefit.

As you may be aware, the US government, the Treasury department, and the Federal reserve Board have concluded plans to change the face of the US $ bills because of counterfeiting as they claim, and the 100 $ bill made its debut since Wednesday, April 21st, 2010.kindly go through the below link to see what am trying to explain to you;

http://news.bbc.co.uk/2/hi/7444083.stm
http://www.cnn.com/2006/WORLD/meast/10/11/iraq.deaths/

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

END