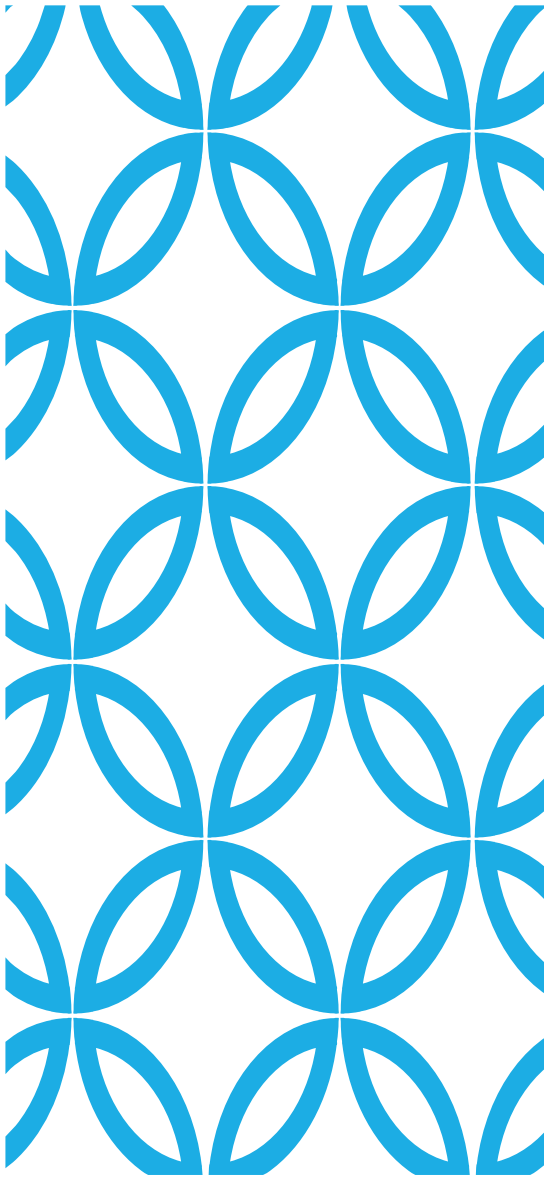


AUTHENTICATION OF PEOPLE

Dr. Nguyen Tuan Nam
nam.nguyen@brumob.com

AUTHENTICATION

Authentication is done differently depending on the capabilities of the thing being authenticated

The two most important capabilities

- Ability to store a high-quality cryptographic key
- Ability to perform cryptographic operations

"High quality key" = secret chosen from a very large space so that computationally infeasible to guess the secret by exhaustive search

Computer has both capabilities

Person has none

USER AUTHENTICATION

3 main techniques to verify that you are who you claim to be

- What you know: passwords
- What you have: ATM cards, physical key
- What you are: biometric devices (voice recognition systems, fingerprint analyzers)

PASSWORDS

Predate computers

- Special greeting

Many problems with using passwords for authentication

- Eavesdropper might see the passwords
- Intruders might read the password information file
- Guess password by making direct login attempts
- May be crackable by an off-line computer search
- Convenience vs. security
  - Authorized users will become enemy if the security mechanism becomes too inconvenient to deal with

ON-LINE PASSWORD GUESSING

- One can impersonate you if they can guess your password
- Many chosen passwords are obvious
  - Name
  - DOB
- Given enough guesses, any password can be guessed
  - Whether it is feasible depends on how many guesses it takes and how rapidly passwords can be tested
  - Military use: wrong password → got shoot

HOW TO PREVENT ON-LINE PASSWORD GUESSING

Work in group

PREVENT ON-LINE PASSWORD GUESSING

- Computer are much faster and more patient than people at making guesses → design the system so that guesses have to be typed by a human
- Keep track of the number of consecutive incorrect passwords for an account
  - When the number exceeds a threshold → lock the account
  - Ex: PINs on ATM cards

PREVENT ON-LINE PASSWORD GUESSING

Slow down a guesser

- Limited number of account/password guesses per connection attempt
- Incorrect passwords to be processes slowly

Catch a guesser

- Trace the connection
- Take corrective action
- Report to users when they log in the time of their previous login and number of unsuccessful password attempts

PREVENT ON-LINE PASSWORD GUESSING

- Expected time to guess password = expected number of guesses / guess rate
- Beside limiting the guess rate, we can ensure the search space is large enough
- Randomly chosen password → inconvenient
- Let user choose their own passwords but warn them to choose good ones and enforce that choice where possible

OFF-LINE PASSWORD GUESSING

Online password guessing

- Guessing can be slowed down and audited

Offline password guessing

- Attacker may obtain a cryptographic hash of the password or a quantity encrypted with the password
- Attacker guess a password, perform the same hash, and compare with the quantity
- No one knows and at a speed limited only by procurable compute power

OFFLINE PASSWORD GUESSING

Publicly readable UNIX password file

- Unaudited and fairly high-performance way of guessing passwords
- Can't look up if user forgets password

Salt

- Stores both the salt and a hash of the combination of the salt and the password

HOW BIG SHOULD A SECRET BE?

- To thwart an online attack, the secret does not have to be chosen from a large space
  - ATM systems have 4 to 6 decimal digits
- Offline attack
  - The secret must be chosen from a very large space → 64 bits

EAVESDROPPING

Risk and prevention?

EAVESDROPPING

Password must be uttered to be used → always chance of eavesdropping

Watch as someone types a password

Wiretap to watch all the passwords (camera, logging devices)

Prevention

Distance

Complex passwords (more fingers involved when typing)

Mask the password

One-time passwords (list)

List of reused password (list can be shorter and used longer)

PASSWORDS AND CARELESS USERS

Password posted on the console

Including passwords online in accessible places

Including passwords in scripts

- Automate access to other systems

Including passwords in messages sent via email, SMS

USING A PASSWORD IN MULTIPLE PLACES

WHAT DO YOU THINK?

DO YOU LIKE IT?

REQUIRING FREQUENT PASSWORD CHANGES

Admin: password changed every 90 days

User resets password to the same thing

Admin: new password must be different from old

User: set to something new, then sets back to the old

Admin: keep track of previous n password

User: n+1 times and set back to the old

Admin: not allows password changed too soon

User: new password similar to old

Admin: forbid that

User: accept impossible-to-remember passwords and post them on their terminal

A LOGIN TROJAN HORSE TO CAPTURE PASSWORDS

INITIAL PASSWORD DISTRIBUTION

- User appears at the terminal of the system admin
- Creates the account and initial strong password and gives it to the user (handed, mailed)

AUTHENTICATION TOKENS

Physical device that person carries around and uses in authenticating → what you have

Must be coupled with one of the other 2 mechanisms to be secure (what you know, what you are)

Several forms

- Keys
- Credit card

Disadvantage

- Requires custom hardware (key slot or card reader) on every access device
- Tokens can be lost or stolen → suplemented with a PIN or password
- Forget tokens at home?

SMART CARD

Size of the credit card but with an embedded CPU and memory

Various forms

- PIN protected memory card
- Cryptographic challenge/response cards
- Cryptographic calculator
  - Readerless smart card
  - Requires no electrical connection to the terminal
  - Has a display and a keyboard

PHYSICAL ACCESS

BIOMETRICS

Retinal scanner

- Examines the tiny blood vessels in the back of your eye
- Expensive and psychologically threatening user interface

Fingerprint readers

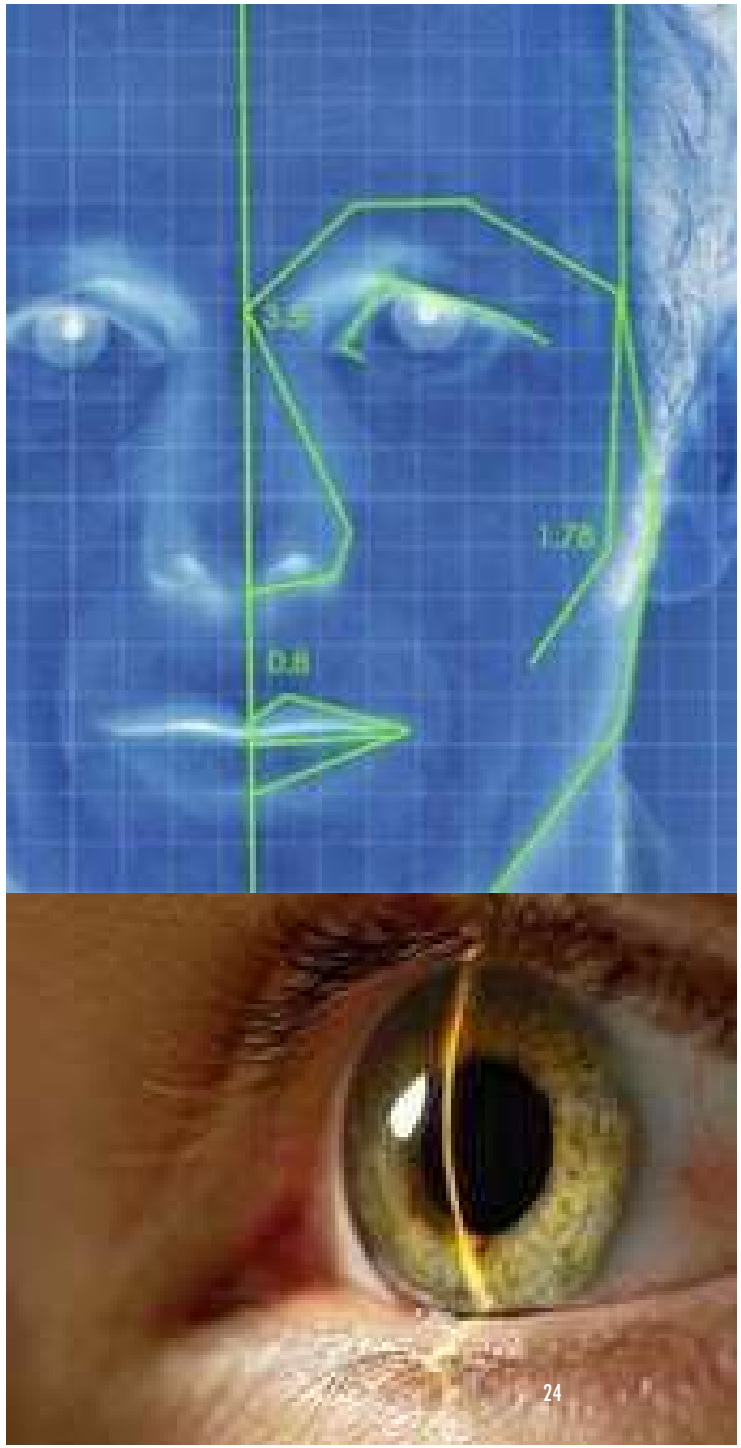
BIOMETRIC DEVICES

Face recognition

- Measure facial dimensions
- Don't show up at work with a black eye and a swollen jaw

Iris scanner

- Maps the distinctive layout of the iris of your eyes



BIOMETRICS

Handprint readers

Voiceprints

Keystroke timing

Signatures