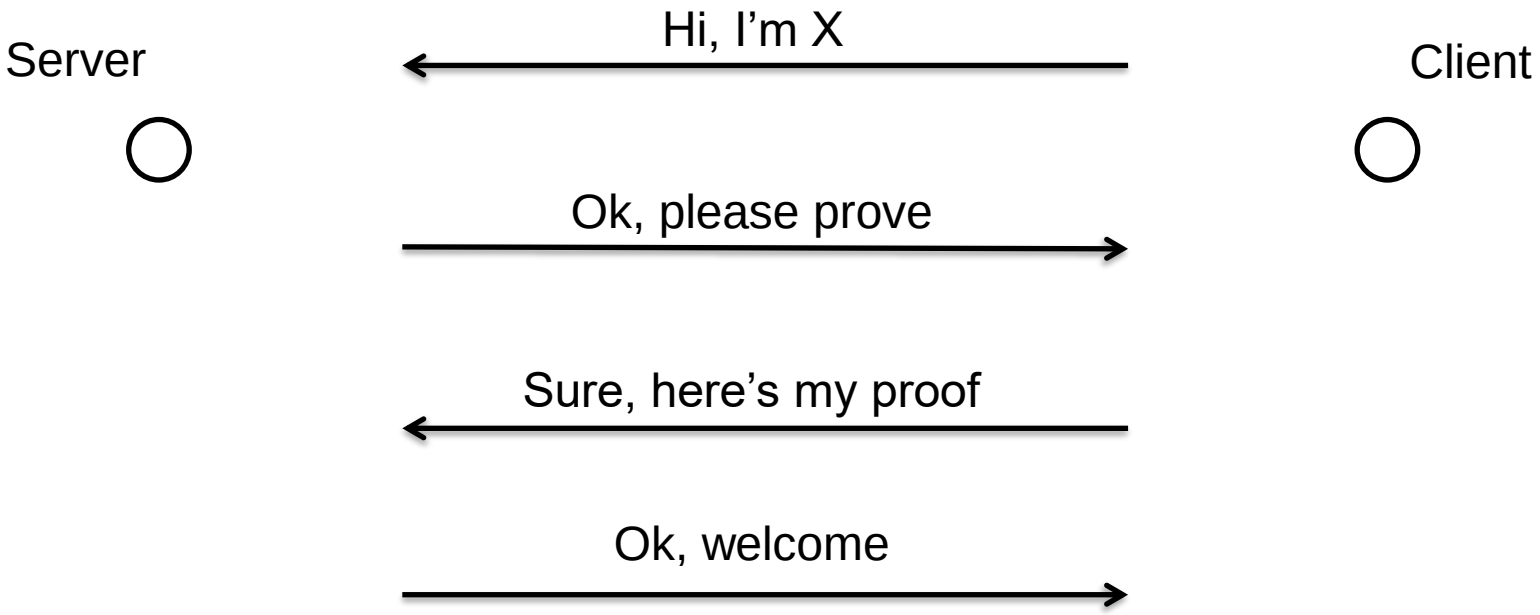
UNIVERSITY OF TWENTE.

Authentication

Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts

WHAT IS AUTHENTICATION? (INFORMAL)



PROVING YOU'RE YOU: FACTORS

Something the user *knows*

Something the user *has*

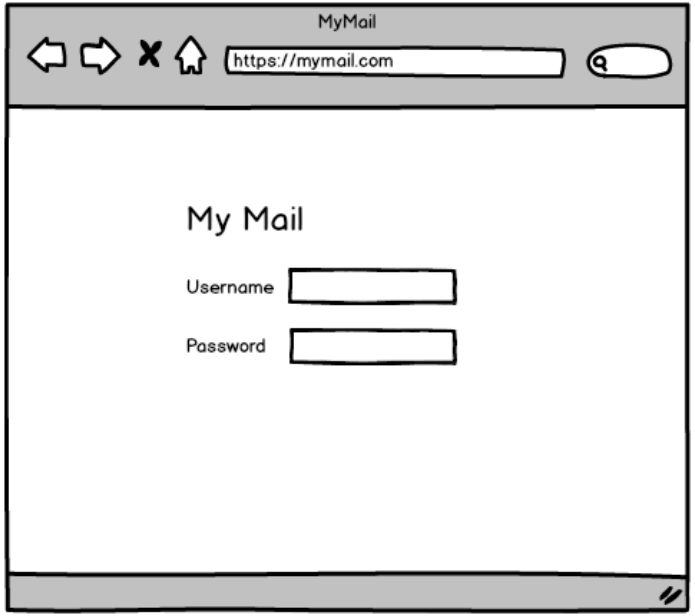
Something the user *is*

Combine for stronger authentication:
Multi-factor authentication

SOMETHING THE USER *KNOWS*

Pincodes,
passwords
&
passphrases

PASSWORDS: THE GOOD



Simple & understandable

Familiar & widespread

Portable

Cheap to implement

PASSWORDS: THE BAD

Re-use across domains

Managing

Too simple passwords

Phishing & sniffing

SOMETHING THE USER *HAS*

Essence:

Having *access* to a secret

Many variants:

Type of secret
- Shared symmetric key
- Private key of a asymmetric key pair

Additional protection
- Separate device
- Tamper-proof hardware (token)
- Pin/password protected

Challenge-response vs. synchronous

RSA SecurID token

- Hardware token
- Tamper-proof
- Synchronous
- Shared symmetric key (seed)
- Sometimes called:
  One Time Password (OTP)

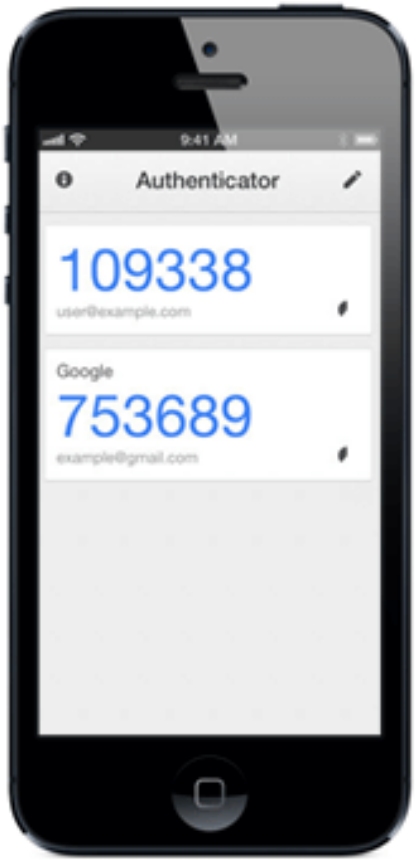
yubico’s YubiKey

- Hardware token
- Tamper-proof
- Synchronous
- Shared symmetric key

http://www.yubico.com/

A bank’s access token

- Hardware token
- Tamper-proof
- Challenge-response
- Shared symmetric key
- Pin-protected



Google Authenticator

- Separate device (mobile)
- Synchronous
- Shared symmetric key

SOMETHING THE USER *IS*

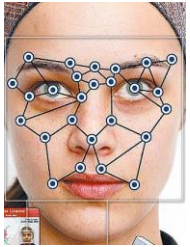
Main idea: using unique personal attributes for authentication

Downsides:

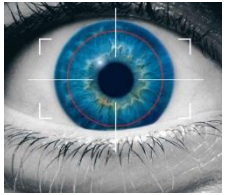
- Intrusive
- Hard to replace
- False positives & negatives
- Complex & expensive

fingerprint

hand geometry



facial scan



iris scan

retina scan

palm scan

voice print

signature dynamics

keyboard dynamics

SECURITY PROPERTIES?

Confidentiality

Integrity

Availability

UNIVERSITY OF TWENTE.

Authentication

Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts