Lecture 8

Thursday, 8 December 2022 14:23

passwords are everywhere

Cryptographic keys are difficult to remember

↓

passwords are shorter and have easier to use

also: password mechanisms are easy to implement

passwords used for:

- local system
- remote login
- web services: email
- HDD encryption e.g. BitLocker

passwords must be

- easy to remember
- hard to guess

→ conflicting

online attack: repeated guessing, trying to login

can deny access after repeated failure

offline attacks: repeated guessing, checking for correctness (unknown e.g. side task is known)

check must be made externally

attack vectors:

interception

- unencrypted login page
- spyware
- ...

password must be transmitted securely

social engineering

- call victim and ask for password
- "educated" guess

users must be cautious w.r.t. passwords

guessing passwords

personal information

- names
- birthdays
- home towns

social engineering

or

brute force

↓

realistic in online attack

literal password

word from a dictionary

still too little entropy / options

obfuscated word

pick random word, apply some transformation rules

a bit more difficult

but still easily doable

XKCD: correct horse battery staple

pick random words

multiple

also called diceware

force node e.g. based on throwing a dice

still easy to enumerate by concatenating words from dictionary

derive password from passphrase → use easy to remember sentence, apply transformations

totally random passwords → difficult to remember → password manager

↓

practically the same as cryptographic key with reformatting