Lab14 - Password Cracking

2025/5/26
By 林煜傑

Credits: 2023 TA 陳亮瑾、2024 TA 楊偉倫

Agenda

- Hash functions
- Password authentication
- Lab - Cracking passwords

Hash Functions

What are hash functions?

- A hash function is a function that map data of arbitrary size to fixed-size values.
- **Hashing != Encryption**

```
uint8_t hash (uint64_t x) {
    return (pow(3, x) * 10) & 0xff
}
```

Applications

- Hash table
- File integrity
- Password Authentication
- Proof-of-work (POW)

Common Hash Functions

- MD5
- CRC-8,16,32,64
- SHA-1
- SHA-2
- SHA-256

Password Authentication

How Are Passwords Stored?

Attempt 1: Plaintext

Store plaintext password in database.

- Terrible
  - Why?

Properties of Hash Functions

- One-wayness
  - Given y, it's computationally infeasible to find x such as y = H(x)
- Weak collision resistance:
  - Given x, it's computationally infeasible to find x' != x such that H(x') = H(x)
- Strong collision resistance
  - It's computationally infeasible to find x and x' such that x' != x and H(x') = H(x)

Attempt 2: hash(password)

Store `hash(password)` in database.

- Better
  - What properties are used?
  - What properties are needed?
- Any problems?

Attempt 3: Salts

Store salt `r` and `hash(password + r)` in database.

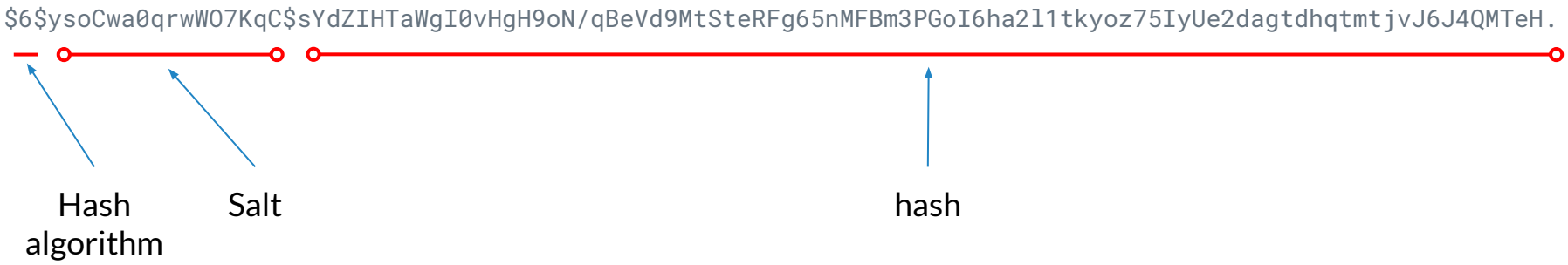
- Even better
- Any problems?

Attempt 4: Multiple Rounds

```
p = password + salt
for (int i = 0; i < round; ++i) {
    p = hash(p)
}
```

Store **p** in database.

Common Format



https://manpages.debian.org/buster/manpages-dev/crypt.3.en.html

Cracking Passwords

- John The Ripper

Tools

- John the ripper
  - https://www.openwall.com/john/
  - We will use this for Lab
- Hashcat
  - https://hashcat.net/hashcat/
- Hydra
  - https://www.hydra-dongle.com/download/

Download John 1.9.0-jumbo-1

- Go to the John the ripper official github repo
- git clone to local
- `cd john/src`
- `./configure`
- `make -j 4`
- `cd ../run`

Command format

- `./john [options] <file of password hash>`
- `./john --help` to see available options

Useful tips

- `john.pot`
  - Saves cracked passwords
  - Can also use option `--show` to show cracked passwords
- Use different cracking modes and limits to speed up cracking
- Use `XXX2john(.YY)` to extract password hashes from encrypted files

Common Cracking Modes

- Dictionary (Wordlist)
- Incremental
- Mask

Length range options

```
--length=N                  Shortcut for --min-len=N --max-len=N
--min-length=N              Request a minimum candidate length in bytes
--max-length=N              Request a maximum candidate length in bytes
--max-candidates=[-]N       Gracefully exit after this many candidates tried.
                            (if negative, reset count on each crack)
--max-run-time=[-]N         Gracefully exit after this many seconds (if negative,
                            reset timer on each crack)
```

Lab

Task: Crack The Zip+PDF

- Download the zip file from here
  - Download task<last digit of your student ID>.zip
- You need to first crack the zip file password
  - Password hint: Dictionary mode
- After unzip the zip file, you need to crack the pdf password
  - Password hint: Contains exactly 5 (Lowercase + Digits)

Task Submission

- Submit form
- Requirements:
  - zip password + success command screenshot
  - pdf password + success command screenshot
  - secret code in pdf