

openHPI course "Digital Identities
Guess, tap, reuse -
Attacks on passwords

Prof. Dr. Christoph Meinel

Hasso Plattner Institute, University of Potsdam

Attacks on passwords

Password-based authentication is often overcome by unauthorized persons using the following methods:

- Password **guessing**
- password **cracking**
 - **Systematic testing**, e.g. with word lists, password top 10 lists, ...
- **Interception of** passwords (sniffing)
 - **Network packets** are intercepted and searched for the presence of user names and passwords
- Use of **keyloggers** and **Trojans that** eavesdrop on the victim system when entering passwords
- **social engineering**

Guessing passwords (1/4)

- Passwords are guessed online and tried directly when trying to gain access to a service on the Internet.
- User/password combination guessing surprisingly often successful because users use too simple passwords and reuse passwords
- Convenience in balancing safety and usability:
 - simple passwords are easy to guess, but also easy to remember ...

Password guessing (2/4)

Find a valid username

Guessing passwords can only be successful if a valid username is found.

- Use of common usernames
 - e.g. admin, guest, service, ...
- Use of usernames from other services
 - e.g. from leaked databases
- Generation of user names according to known patterns
 - many use first and/or last name as username
 - add numbers at the end
 - e.g. John64, Robert17, ...
 - E-mail addresses, ...

Password guessing (3/4)

Finding valid passwords

To make passwords easier to remember, many users choose passwords with a simple structure:

- Studies show that about 10% of all users choose their first name as their password.
- Unchanged default settings of user/password combinations (default) are also used, with which systems are delivered or which are listed in the manual (example: private WLAN routers).
 - e.g. test/test, guest/guest, admin/admin
- Hackers can easily try out lists with frequent combinations...

Guessing passwords (4/4)

Various studies on password security show:

- 20-40% of passwords in a database can be guessed
- The first user/password combination can usually be found within the first 15 minutes.
- Current password crackers can test approx. 1500 user/password combinations per minute on websites

Quick guessing becomes possible because many passwords are too easy to choose

- Despite warnings passwords are chosen too simply out of carelessness!

Crack passwords (1/6)

The so-called cracking of passwords is executed offline on a list of hashed passwords

Target:

- derive passwords in plain text from their obfuscated hash values
- Is often much faster than guessing passwords

Prerequisite:

- Obtaining a file with password hashes
- e.g. from leakter database or cracked computer

Password cracking (2/6)

The cracking is carried out either with the help of **dictionaries** or via **Brute Force** (by "brute force").

- **dictionary**

- Lists of dictionary entries are hashed one after the other
- Hashes are compared with the existing password hash.

- **Brute Force**

- All possible character combinations are tried out
- Brute force attacks find the password in any case - but take far too long (decades, centuries, ...) if the password is long enough.

Password cracking (3/6)

- Password cracking programs are very fast because they use both the processor(s) and graphics processor(s) of a computer.
- Rates is always dependent on network bandwidth and vulnerable to disruptions and delays
- Historical development:
 - 40 years ago three passwords per second could be tested (DEC-PDP-11)
 - today: per second can be
 - Test approx. 3 billion SHA1 passwords on current PCs
 - Approximately 200 billion MD5 passwords using clusters of GPUs

Password cracking (4/6)

- Speed at password cracking depends strongly on hardware used: processor (CPU), graphics processor (GPU)
- GPUs are extremely efficient at password cracking
 - Optimized for parallel mathematical calculations
 - Partly 1000x faster than processors
- Duration to crack at 100 billion tests (with special hardware) per second:

password	time	password	time
secret	< 1 second	secret12	29 seconds
! sEcRe!	5,41 minutes	secret2	1,45 hours
!sEcRe!2	18.62 hours	sEcRe!2%9	19.24 years

Sync by honeybunny <https://www.g>

Password cracking (5/6)

There are several free **tools to crack passwords**

- very famous are **John the Ripper** and **Hashcat**. They support the cracking of all common password hash methods, such as DES, MD5, SHA-1, Blowfish, ...
- **RainbowCrack** supports efficient cracking with pre-calculated Rainbow tables
 - Only for hash functions without the use of Salts
- **L0phtCrack** is known for efficient cracking of Windows passwords

Password cracking (6/6)

Attention:

- Good passwords are useless if infiltrated eavesdropping programs can listen in to every keystroke.

Recommendation:

- Test your own passwords against freely available word lists, e.g. from

<http://www.openwall.com/john/> - sync:βÇ
 ÊâÊâ

<http://www.openwall.com/wordlists/> - pro
 udly presents

<http://www.oxfordwordlist.com/> - proudly
 presents

<https://www.grc.com/haystack.htm> Sync by honeybunny

Interception of passwords (sniffing)

- Another method for obtaining user names and passwords is interception or eavesdropping - **sniffing**, e.g. by eavesdropping and analyzing network packets in local (LAN) or wireless networks (WLAN).

Tools:

- Freely available tools: Wireshark, tcpdump, ...

Basic idea:

- Content of (unencrypted) data packets can be easily analyzed and filtered by terms such as "login" or "password"

spying out passwords

Installation of small malicious programs - **keyloggers** - for intercepting keystrokes and saving them in a special file, if they are in the context of text entries such as "login..." or "passw...".

- Hackers can later download files from the system or have them automatically sent to a central server (drop zone) and store them there.

Summary: Attacks on passwords

- Attackers have numerous possibilities to obtain passwords:
 - **Guessing** passwords
 - **Crack** stolen password hashes
 - Interception of network packets (**sniffing**)
 - Use of **software** (keyloggers, Trojans)
 - **social engineering attacks**

Summary: Attacks on passwords

- Attackers have numerous possibilities to obtain passwords:
 - **Guessing** passwords
 - **Crack** stolen password hashes
 - Interception of network packets (**sniffing**)
 - Use of **software** (keyloggers, Trojans)
 - **social engineering attacks**