Password Cracking
(using Rainbow Tables)
Password Storage

Approaches

Implementations
Password Storage

- Cannot store password in plain text.
- Cryptographic Hash are stored.
- While authenticating, password is converted to hash and hash compared.
Password Storage

- Password (cleartext) `"hello"
- Hash function
- Hashed password
- Password store

```
$1$r6T8SUB9$Qxe41FJyF/3gkPluvKOQ90
```
Approaches

- Brute Force Attack
- Dictionary Attack
- Rainbow Table Attack
Brute Force Attack

- A brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly.
- The attacker systematically checks all possible passwords and passphrases until the correct one is found.
- This is as an exhaustive search.
- Take too long. (for longer passwords)
- Becomes exponentially more difficult to crack.
Brute Force Attack

```plaintext
C:\bin\ighashgpu>ighashgpu.exe /h:e99a18c428cb38d5f260853678922e03 /t:md5 /c:sd /min:6 /max:6  
**********************************************************************************  
*** MD4/MD5/SHA1 GPU Password Recovery v0.62 *** 
*** For ATI RV 7X0 cards and nVidia 'CUDA' ones (G80+) *** 
*** (c) 2009 Ivan Golubev, http://golubev.com *** 
*** see "readme.htm" for more details ***  
**********************************************************************************  
*** Any commercial use of this program is strictly forbidden ***  

Found 1 CAL device(s) 
Starting brute-force attack, CharSet Len = 36, Min passlen = 6, Max passlen = 6 
Charset (unicode -> 0) [abcdefghijklmnopqrstuvwxyz0123456789] 
Charset in HEX: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 30 31 32 33 34 35 36 37 38 39 
Starting from [aaaaaaaa] 
Hash type: MD5, Hash: e99a18c428cb38d5f260853678922e03 
Device #0: [RV7x0] 750.00 Mhz 800 SP 
Hardware monitoring enabled, threshold temperature is 90°C. 
CURPWD: 2ru329 DONE: 80.94% ETA: 0s AVRSPD: 1158.0M 
Found password: [abc123], HEX: 61 62 63 31 32 33 
Processed 1 769 996 288 passwords in 2s. 
Thus, 1 146 370 652 password(s) per second in average. 

C:\bin\ighashgpu>
```
Dictionary Attack

- Dictionary attack uses a wordlist that contains words, phrases, common passwords and other strings that can used as a password.
- The password is cracked after comparing every word in the wordlist (after hashed) to the password hash.
- These files are also containing words with appending numbers to the end of them (e.g. “harrys123”) and with their leet speak equivalent ("harrys" becomes ”h4rry5”).
- Although, dictionary attacks have a fairly high speed, are ineffective against passwords that are not based on a dictionary word.
Dictionary Attack

Figure 12-2  Dictionary attack
Rainbow Tables

- A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes.

- Practical example of space - time tradeoff. (less computer processing time and more storage)

- A single chain represented by a Plain Text (Starting Point - P1) and another Plain Text (Ending Point - P2) can represent multiple Hashes in between.

- Multiple Reduction Functions are used to avoid merging of chains.
Creation of hash chains
Simplified rainbow table with 3 reduction functions
Sequential Implementation

- We implement ‘X’ Number of chains with ‘Y’ Number of [P] elements
- Implementing R[1] .. R[Y-1] related reduction functions and equal number of H()
- Total Operations on single core will be around \( (X \times R[1..Y-1] \times H[1..Y-1]) \)
- While searching for the corresponding plain text value [P-password] of a hash [H(P)]; searching process will consider each chain one by one.
Parallel Implementation

- We implement ‘X’ Number of chains with ‘Y’ Number of [P] elements
- Implementing R[1] .. R[Y-1] related reduction functions and equal number of H()
- Total Operations on single core will be around \((X \times R[1..Y-1] \times H[1..Y-1]) / K\); if we use k cores for computing.
- While searching for the corresponding plain text value [P-password] of a hash [H(P)]; searching process will distribute hash chains to several available threads.
THANK YOU
Q&A