Authentication Technologies Security Technologies

Submitted to:
Lecturer Vaibhav Mittal

Submitted by:
Syed Rahman

Table of Contents

Introduction

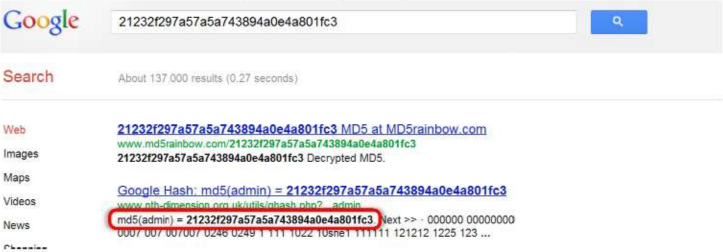
To have a good authentication technique requires the need of studying the ways it can be broken, which was the goal of this practical. We learnt various password cracking techniques using various tools which gave us the idea as which password is weak and which is strong. We also learned how to send a digitally signed and encrypted email for secure communication and the precautions involved in that.

Achievements of the practical

- Able to crack password hashes of different types.
- Establishing secure communication via email.
- Using rainbow tables to crack multiple hashes.
- Studied the techniques, power and limitations of 'John the Ripper' tool.

TASK 1: BASIC PASSWORD HASH CRACKING

- Search Google to obtain plaintext passwords for pre-computed hashes.



21232f297a57a5a743894a0e4a801fc3

Search

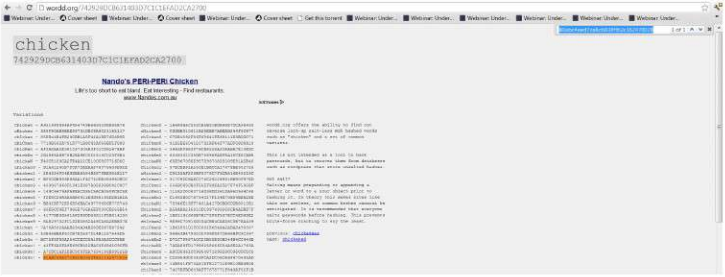
About 137,000 results (0.27 seconds)

21232f297a57a5a743894a0e4a801fc3 MD5 at MD5rainbow.com
www.md5rainbow.com/21232f297a57a5a743894a0e4a801fc3
21232f297a57a5a743894a0e4a801fc3 Decrypted MD5.

Google Hash: md5(admin) = 21232f297a57a5a743894a0e4a801fc3
www.nth-dimension.org.uk/utils/ghash.php?...admin
md5(admin) = 21232f297a57a5a743894a0e4a801fc3. Next >> · 000000 00000000 0007 007 007007 0246 0249 1 111 1022 10sne1 111111 121212 1225 123 ...

Figure 1.1.1: A very common password, revealed easily by Google.

- Searching the hash with Google returned a page with password hashes of 'chicken' and its variants.



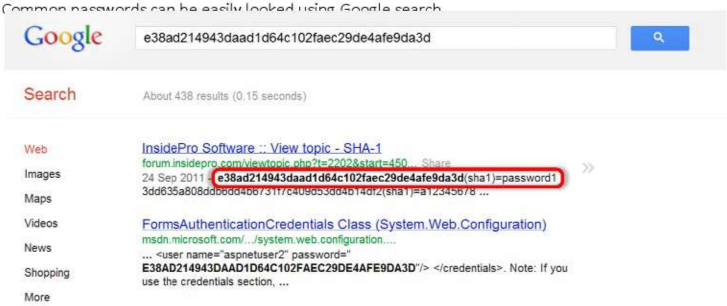
wordd.org/742929DCB631403D7C1C1EFAD2CA2700

chicken
742929DCB631403D7C1C1EFAD2CA2700

Nando's PERI-PERI Chicken
Life's too short to eat bland. Eat Interesting - Find restaurants.
www.Nandos.com.au

Figure 1.1.2: The password is a variant of the string 'chicken'.

- Common passwords can be easily looked using Google search



About 438 results (0.15 seconds)

InsidePro Software :: View topic - SHA-1
forum.insidepro.com/viewtopic.php?t=2202&start=450... Share
24 Sep 2011 – **e38ad214943daad1d64c102faec29de4afe9da3d**(sha1)=password1 3dd635a808ddb6dd4b67311c409d53dd4b14df2(sha1)=a12345678 ...

FormsAuthenticationCredentials Class (System.Web.Configuration)
msdn.microsoft.com/.../system.web.configuration....
... <user name="aspnetuser2" password=" **E38AD214943DAAD1D64C102FAEC29DE4AFE9DA3D**"/> </credentials>. Note: If you use the credentials section, ...

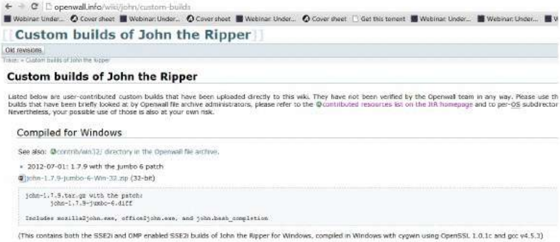
Figure 1.1.3: First search result in Google gives the password string.

HASH	Hash Type	Password (without quotes)
21232f297a57a5a743894a0e4a801fc3	**RAW-MD5 (16 bytes)**	**'admin'**
80abc4eed7ce8cb038ffb2c162470028	**RAW-MD5 (16 bytes)**	**'ch1ck3n!'**
e38ad214943daad1d64c102faec29de4afe9da3d	**RAW-SHA-1(20 bytes)**	**'password1'**

Table 1.1: Passwords and Hash types for cracked hashes

TASK 2: PASSWORD HASH CRACKING USING *JOHN THE RIPPER*

- To crack more complex passwords or salted passwords we can use tools like *John the Ripper*, which provide an automatic process of breaking the password hashes.



[[Custom builds of John the Ripper]]

Custom builds of John the Ripper

Listed below are user-contributed custom builds that have been uploaded directly to this wiki. They have not been verified by the Openwall team in any way. Please use th builds that have been briefly looked at by Openwall file archive administrators, please refer to the contributed resources list on the JtR homepage and to per-OS subdirector Nevertheless, your possible use of those is also at your own risk.

Compiled for Windows

See also: contrib/win32/ directory in the Openwall file archive.

- 2012-07-01: 1.7.9 with the jumbo 6 patch

john-1.7.9-jumbo-6-Win-32.zip (32-bit)

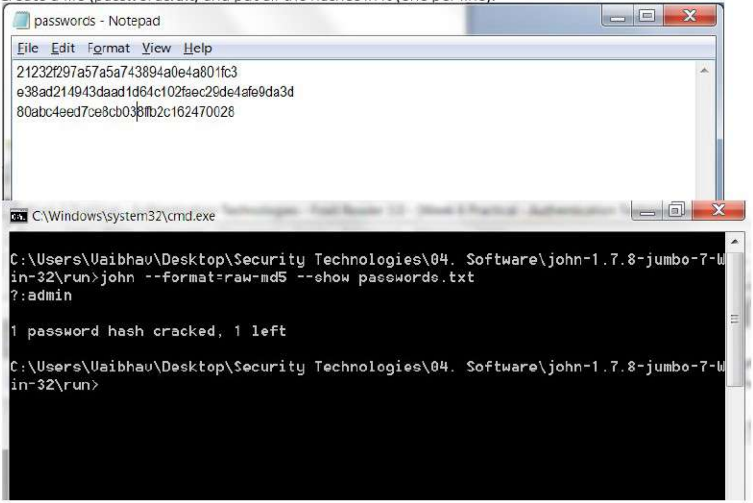
```
john-1.7.9.tar.gz with the patch:
        john-1.7.9-jumbo-6.diff

Includes mozilla2john.exe, office2john.exe, and john.bash_completion
```

(This contains both the SSE2i and OMP enabled SSE2i builds of John the Ripper for Windows, compiled in Windows with cygwin using OpenSSL 1.0.1c and gcc v4.5.3)

Figure 1.2.1: Download John the Ripper Custom Build version.

- Create a file (passwords.txt) and put all the hashes in it (one per line).



```
21232f297a57a5a743894a0e4a801fc3
e38ad214943daad1d64c102faec29de4afe9da3d
80abc4eed7ce8cb038ffb2c162470028
```

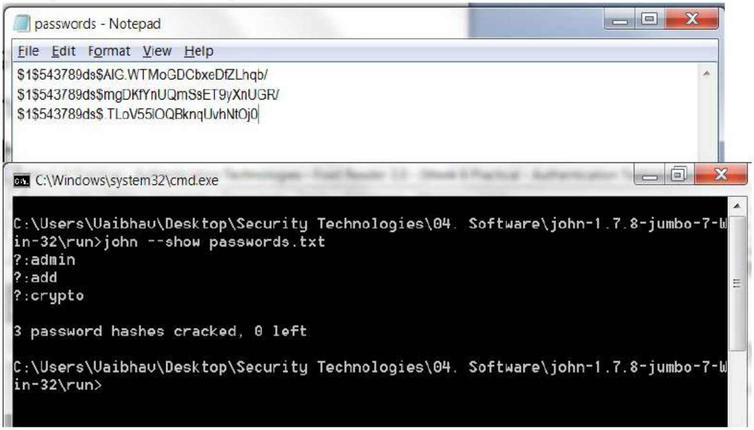
```
C:\Users\Vaibhav\Desktop\Security Technologies\04. Software\john-1.7.8-jumbo-7-W
in-32\run>john --format=raw-md5 --show passwords.txt
?:admin

1 password hash cracked, 1 left

C:\Users\Vaibhav\Desktop\Security Technologies\04. Software\john-1.7.8-jumbo-7-W
in-32\run>
```

Figure 1.2.2: Cracking easy passwords using John the Ripper.

- Now try to crack shadow salted passwords.



```
$1$543789ds$AIG.WTMoGDCbxeDfZLhqb/
$1$543789ds$mgDKfYnUQmSsET9yXnUGR/
$1$543789ds$.TLoV55lOQBknqUvhNtOj0
```

```
C:\Users\Vaibhav\Desktop\Security Technologies\04. Software\john-1.7.8-jumbo-7-W
in-32\run>john --show passwords.txt
?:admin
?:add
?:crypto

3 password hashes cracked, 0 left

C:\Users\Vaibhav\Desktop\Security Technologies\04. Software\john-1.7.8-jumbo-7-W
in-32\run>
```

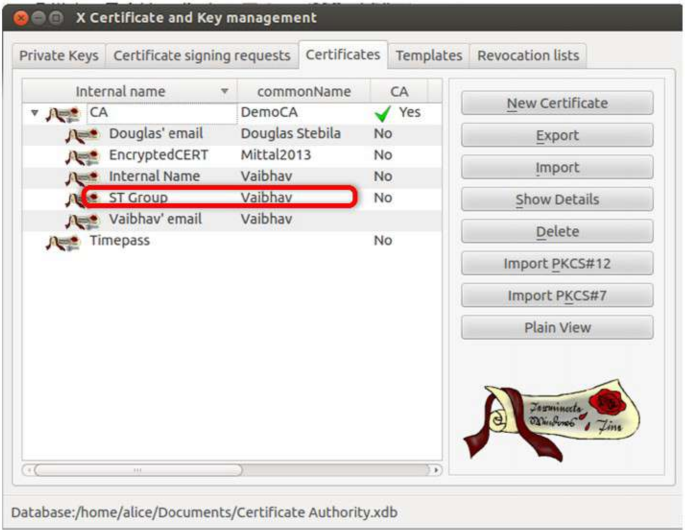
Figure 1.2.3: All salted passwords successfully cracked in real time.

HASH	Hash Type	Password (without quotes)	SALT
$1$543789ds$AIG.WTMoGDCbxeDfZLhqb/	**FreeBSD MD5 (salted)**	**'admin'**	**543789ds**
$1$543789ds$mgDKfYnUQmSsET9yXnUGR/	**MD5 (salted)**	**'add'**	**543789ds**
$1$543789ds$.TLoV55IOQBknqUvhNtOj0	**MD5 (salted)**	**'crypto'**	**543789ds**

Table 2.1: Passwords, Hash types and Salts for cracked hashes

TASK 3: SECURE EMAIL

- Issue a new certificate from inside the CA..

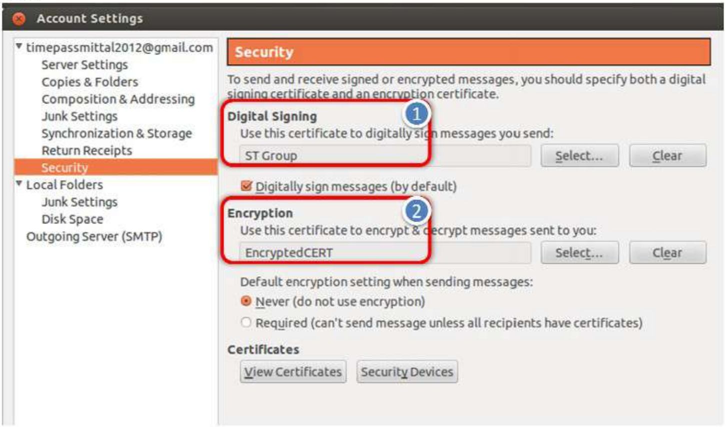


Internal name	commonName	CA
CA	DemoCA	✓ Yes
Douglas' email	Douglas Stebila	No
EncryptedCERT	Mittal2013	No
Internal Name	Vaibhav	No
ST Group	Vaibhav	No
Vaibhav' email	Vaibhav	
Timepass		No

Database:/home/alice/Documents/Certificate Authority.xdb

Figure 1.3.1: Create new certificates.

- Use one certificate for signing (ST Group) and another for encrypting (EncryptedCERT) the email.



Account Settings

Security

To send and receive signed or encrypted messages, you should specify both a digital signing certificate and an encryption certificate.

Digital Signing

Use this certificate to digitally sign messages you send:

ST Group

☑ Digitally sign messages (by default)

Encryption

Use this certificate to encrypt & decrypt messages sent to you:

EncryptedCERT

Default encryption setting when sending messages:

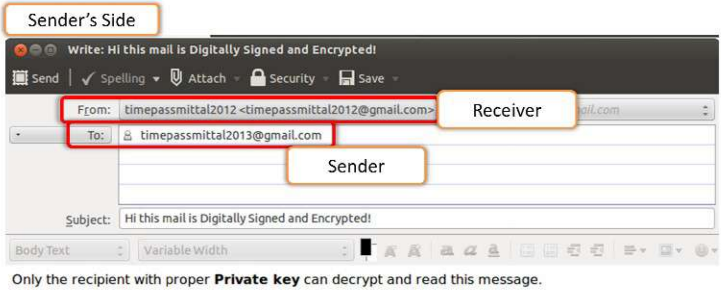
● Never (do not use encryption)

○ Required (can't send message unless all recipients have certificates)

Certificates

Figure 1.3.2: Using Modify Headers to change the Referrer and Host parameters

- Send a Digitally Signed and Encrypted email to the receiver.



Write: Hi this mail is Digitally Signed and Encrypted!

From: timepassmittal2012 <timepassmittal2012@gmail.com>

To: timepassmittal2013@gmail.com

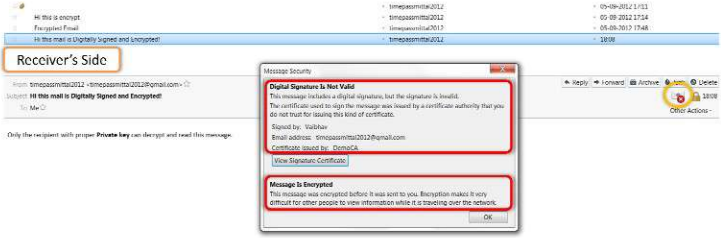
Subject: Hi this mail is Digitally Signed and Encrypted!

Only the recipient with proper **Private key** can decrypt and read this message.

Figure 1.3.3: Sender sends a digitally signed and encrypted email to the receeipient.

.

- **Receiver having the pre-shared private key (by secure means) receives the email and is successfully able to decrypt it.**



	timepassmittal2012	05-09-2012 17:11
Hi this is encrypt	timepassmittal2012	05-09-2012 17:14
Encrypted Email	timepassmittal2012	05-09-2012 17:48
Hi this mail is Digitally Signed and Encrypted!	timepassmittal2012	18:08

Receiver's Side

From: timepassmittal2012 <timepassmittal2012@gmail.com>

Subject: **Hi this mail is Digitally Signed and Encrypted!**

To: Me

Only the recipient with proper **Private key** can decrypt and read this message.

Message Security

Digital Signature Is Not Valid

This message includes a digital signature, but the signature is invalid.

The certificate used to sign the message was issued by a certificate authority that you do not trust for issuing this kind of certificate.

Signed by: Vaibhav

Email address: timepassmittal2012@gmail.com

Certificate issued by: DemoCA

Message Is Encrypted

This message was encrypted before it was sent to you. Encryption makes it very difficult for other people to view information while it is traveling over the network.

Figure 1.3.4: Message security confirms that the email is digitally signed and encrypted.

Answer 2.a

Yes, it is a more secure password than the other two.

Explanation:

'ch1ck3n!' takes more time to crack as it is a mixture of

- Lowercase alphabets
- Special characters
- Numbers

While the other two passwords 'admin' and 'password1' only contain lowercase alphabets and numbers.

Since the cracker has to look into more characters it makes it harder to break the 'ch1ck3n!' password and therefore it makes it more secure than the other two.

Answer 2.b

Generate Rainbow Tables with a salt value which is same for all passwords.

Then use a program like RainbowCrack to crack the passwords much faster. However, the time for generating the required Rainbow Tables must also be taken into account.

Answer 2.c

As you don't have the private key to decrypt our encrypted passwords.

Explanation

As the private key necessary to decrypt the message is included in the certificate. The sender and receiver must exchange these certificates (or Private keys) through a secure channel. (may be through a USB drive by meeting personally).

After the receiver has installed the digital certificate in his email client he can decrypt the messages coming from the sender.

Answer 2.d

i) **Secure Token breaks:** If the secure token breaks then also the signing key is password protected (.p12), but if the attacker manages somehow to crack that password as well then also he won't be able to use the key to send a signed certificate as that key was specifically generated for a particular email. The attacker can modify a message sent by the legitimate user and sign it using the acquired key to make it look authentic.
To be on a safer side it's best to revoke all the certificates issued by that key

ii) **Infected PC:** If the computer is infected by a malware then it's very much possible that the attacker can bypass all the security measures of the key and use it to send unauthorised or modified messages.
User *must* revoke all the certificates immediately.

Revoking a Certificate

The certificate manager keeps the record of all the certificates issued. It keeps these records in the form of Certificate Revocation Lists, which can be used to select and revoke any certificate only by the administrator.

Answer 2.e

Self Signed certificate (Wikipedia, 2012): When a user creates a certificate and signs it himself (i.e. with his own private key) then it is called a self signed certificate.

It is also called an Identity certificate as it certifies the identity of the same person.

Applications of Self Signed certificate

The highest ranking CA's certificate (root certificate) can't be verified by any other CA and hence that certificate can only be self signed. Note that it requires a complete trust towards root CA authority.

In a web of trust certificate scheme, where there is no central CA and identity certificate for each user can be self signed. However, this identity can be confirmed by verifying the signatures of other people in the same group who have signed that certificate as well.

Self signed certificates depend on complete trust and otherwise don't make much sense as an attacker can also send a forged self signed message.

Answer 3: Product/ Tool

RainbowCrack (RainbowCrack Project, 2012)

Introduction

RainbowCrack uses time-memory trade-off technique to crack hash' of password(s). It also increases the password cracking speed by using the Graphics Processing Unit (GPU) of the computer.

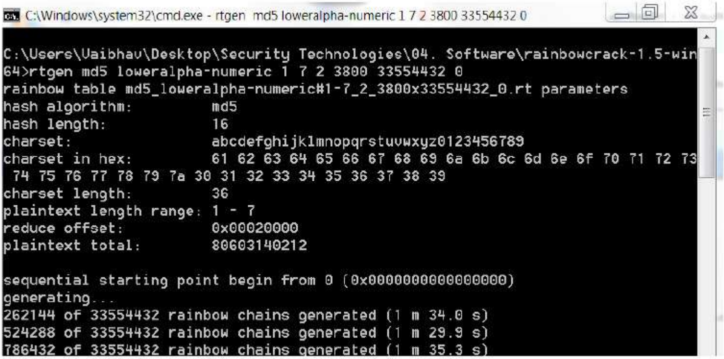
Features

Some of the features of RainbowCrack as listed on its website. (project-rainbowcrack.com)

- "Full time-memory trade-off tool suites, including ***rainbow table generation***, sort, conversion and *lookup*
- Support rainbow table of ***any hash algorithm***
- Support rainbow table of any charset
- Support rainbow table in raw file format (.rt) and compact file format (.rtc)
- Computation on multi-core processor support
- Computation on GPU (via NVIDIA CUDA technology) support
- Computation on multi-GPU (via NVIDIA CUDA technology) support
- Runs on 32-bit Windows operating systems
    - Windows XP 32-bit
    - Windows Vista 32-bit
    - Windows 7 32-bit
- Runs on 64-bit Windows operating systems
    - Windows XP 64-bit
    - Windows Vista 64-bit
    - Windows 7 64-bit
- Runs on 32-bit Linux operating systems (x86 only)
- Runs on 64-bit Linux operating systems (x86_64 only)
- Unified rainbow table file format on all supported operating systems
- Command line user interface
- Graphics user interface (Windows only)"

Usage

1) Generate Rainbow Tables using the rtgen utility in the software package.


C:\Windows\system32\cmd.exe - rtgen md5 loweralpha-numeric 1 7 2 3800 33554432 0

```
C:\Users\Vaibhav\Desktop\Security Technologies\04. Software\rainbowcrack-1.5-win
64>rtgen md5 loweralpha-numeric 1 7 2 3800 33554432 0
rainbow table md5_loweralpha-numeric#1-7_2_3800x33554432_0.rt parameters
hash algorithm:         md5
hash length:            16
charset:                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
charset length:         36
plaintext length range: 1 - 7
reduce offset:          0x00020000
plaintext total:        80603140212

sequential starting point begin from 0 (0x0000000000000000)
generating...
262144 of 33554432 rainbow chains generated (1 m 34.0 s)
524288 of 33554432 rainbow chains generated (1 m 29.9 s)
786432 of 33554432 rainbow chains generated (1 m 35.3 s)
```

Figure 3.1.1: Generating lower case alphabet with numbers Rainbow Tables using rtgen.

Rainbow tables can be generated for dirferrent hash types (MD5, NTLM etc.) and for different character sets.
Example: lowercase alphabet with numbers, mixed case alphabets with numbers etc.
Following syntax can be used to generate desired Rainbow Tables (RainbowCrack Project Tutorial, Step1, 2012):

```
rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index
```

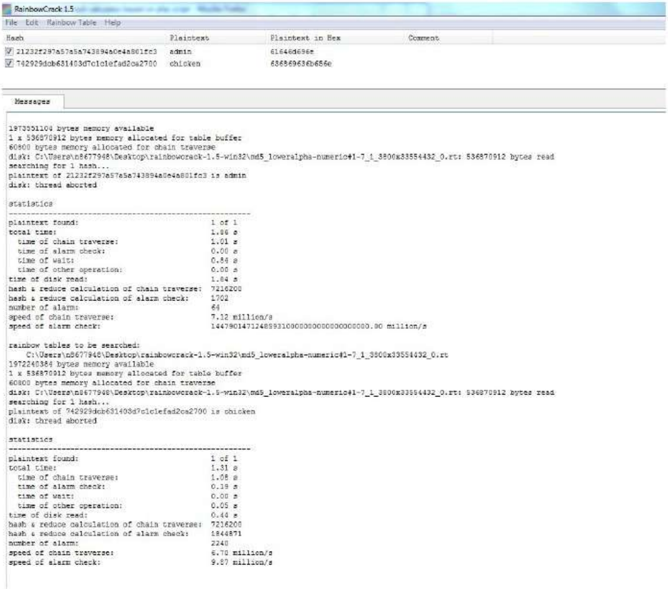
Statistics for Rainbow Table generation on an Intel E8500 Core2Duo processor (3.16 GHz), with 4GB RAM and Windows 7 (64-bit) operating system.

Average Time Taken: 25 hours 48 minutes (for one computer)

NOTE: The tables were generated in parts, simultaneously on 6 computers having the same configuration. By this technique you can save some time if you have access to multiple computers (Average time taken/6 = *4 hours 18 minutes*).

2) Sort the tables using rtsort which sorts the "end point" of all rainbow chains in a rainbow table.
3) Use the GUI tool to load hashes from a pwdump file or insert hashes manually.

4) Select the tables you want to use in the cracking process (tables generated in Step 1) and start cracking.



Hash	Plaintext	Plaintext in Hex	Comment
☑ 21232f297a57a5a743894a0e4a801fc3	admin	61646d696e	
☑ 742929dcb631403d7c1c1efad2ca2700	chicken	636869636b656e	

```
1973551104 bytes memory available
1 x 536870912 bytes memory allocated for table buffer
60800 bytes memory allocated for chain traverse
disk: C:\Users\n8677948\Desktop\rainbowcrack-1.5-win32\md5_loweralpha-numeric#1-7_1_3800x33554432_0.rt: 536870912 bytes read
searching for 1 hash...
plaintext of 21232f297a57a5a743894a0e4a801fc3 is admin
disk: thread aborted

statistics
-------------------------------------------------------
plaintext found:                          1 of 1
total time:                               1.86 s
  time of chain traverse:                 1.01 s
  time of alarm check:                    0.00 s
  time of wait:                           0.84 s
  time of other operation:                0.00 s
time of disk read:                        1.84 s
hash & reduce calculation of chain traverse: 7216200
hash & reduce calculation of alarm check:    1702
number of alarm:                          64
speed of chain traverse:                  7.12 million/s
speed of alarm check:                     1447901471248593100000000000000000000.00 million/s

rainbow tables to be searched:
    C:\Users\n8677948\Desktop\rainbowcrack-1.5-win32\md5_loweralpha-numeric#1-7_1_3800x33554432_0.rt
1972240384 bytes memory available
1 x 536870912 bytes memory allocated for table buffer
60800 bytes memory allocated for chain traverse
disk: C:\Users\n8677948\Desktop\rainbowcrack-1.5-win32\md5_loweralpha-numeric#1-7_1_3800x33554432_0.rt: 536870912 bytes read
searching for 1 hash...
plaintext of 742929dcb631403d7c1c1efad2ca2700 is chicken
disk: thread aborted

statistics
-------------------------------------------------------
plaintext found:                          1 of 1
total time:                               1.31 s
  time of chain traverse:                 1.08 s
  time of alarm check:                    0.19 s
  time of wait:                           0.00 s
  time of other operation:                0.05 s
time of disk read:                        0.44 s
hash & reduce calculation of chain traverse: 7216200
hash & reduce calculation of alarm check:    1844871
number of alarm:                          2240
speed of chain traverse:                  6.70 million/s
speed of alarm check:                     9.87 million/s
```

Figure 3.1.2: Passwords cracked using RainbowCrack

Why this tool?

- RainbowCrack provides a faster way of cracking the hashed passwords by using a time-memory trade-off technique (Rainbow Tables). (John the Ripper does not)
- Facilitates own customised rainbow table generation. (JTR and Ophcrack does not)
- Supports GPU cracking to increase the speed of attack.

Who should use this tool?

- Can be used by *system administrators*, *IT Security personnel* and *consultants* for security auditing and to identify weak passwords.
- Can be used as a password recovery tool by anyone.
- Can be used as an attacking tool to break into networks or systems by an attacker.

Limitations

- Does not support salted hashes.
- Only supports Nvidia graphics card for GPU cracking (ATI not yet supported).
- No support for *Wordlists*.

Answer 3: ACADEMIC PAPER

Altered Fingerprints: Analysis and Detection (Yoon, et al., 2012)

This paper analyses the problems of current Automated Fingerprint Identification Systems (AFIS) which is widely used by law enforcement and border control agencies. It also suggests an algorithm to rectify these problems.

The paper gives some case studies where individuals were found to have altered their fingerprints for circumventing AFIS, staring from the year 1933 to 2010.

It determines the effect of fingerprint alteration on the accuracy of a commercial fingerprint matcher (NFIQ) and finds that the AFIS was unable to match most of the altered fingerprints to the correct person.

Classification of Alterations:

1) **Obliteration:** ridge patterns on fingertips can be obliterated by abrading, cutting, burning applying strong chemicals and transplanting smooth skin.

2) **Distortion:** ridge patterns on fingertips can be turned into unnatural ridge patterns by removing portions of skin from a fingertip and placing them back in different positions.

3) **Imitation:** Removal of a portion of skin followed by exquisite transplantation from other friction ridge skin (skin from other hand). A very successful method, and has deceived AFIS.

The NFIQ algorithm is not suitable for detecting altered fingerprints, especially the distortion and imitation types.

The paper proposes the automatic detection of altered fingerprints by analyzing orientation field and minutiae distribution. See Figure 3.2.1

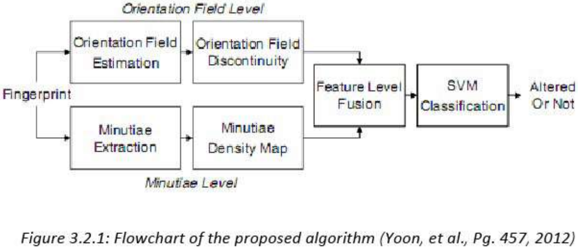


Figure 3.2.1: Flowchart of the proposed algorithm (Yoon, et al., Pg. 457, 2012)

The proposed algorithm satisfies the three essential requirements for alteration detection algorithm:

1) Fast operational time

2) High true positive rate at low false positive rate

3) Ease of integration into AFIS.

The technique was tested on a large database and the results were good as the false positives were only .3%.

The technique does sound effective and can be used to prevent many frauds and crimes which try to evade the automated authentication technologies.

This paper also gives the picture that the biometric authentication systems are now evolving and in coming future will be the main mode of identity verification. Although we must keep in mind that the medical science is also advancing simultaneously and such biometrics authentications may be evaded by the future developments in plastic or cataract surgery.

Conclusion

- We learned about various password cracking techniques based on brute force, wordlists and rainbow tables.

- I explored various tools in this area such as John the Ripper, RainbowCrack, Ophcrack, Trinity Rescue Kit (Windows password recovery) and Advanced Password Recovery (Multi utility password cracker).

- We saw how an attacker can crack weak passwords very easily using such a tool which tells us the ***importance of choosing a strong password.***

- We learnt about setting up a secure email conversation by using Digital Signatures and Encryption.

- We explored the latest developments in the field of Biometric authentication technologies by analysing a recent academic paper.

Reference List

1. RainbowCrack Project, 2012. ***RainbowCrack Project – Crack Hashes with Rainbow Tables.*** [online] Available at: <http://www. project-rainbowcrack.com/> [Accessed 3 September 2012].

2. RainbowCrack Project Tutorial, 2012. ***RainbowCrack Project –RainbowCrack Tutorial.*** [online] Available at: < http://project-rainbowcrack.com/tutorial.htm> [Accessed 4 September 2012].

3. Wikipedia, 2012. ***Self-signed certificate***. [online] Available at: <http://en.wikipedia.org/wiki/Self-signed_certificate> [Accessed 9 September 2012].

4. Yoon Soweon, Feng Jianjiang, Jain Anil K., 2012. ***Altered Fingerprints: Analysis and Detection.*** IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 34, No. 3, pp. 451-464, March 2012, Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6136517>.