Think you have a strong password? Hackers crack 16-character passwords in less than an HOUR

- **During an experiment for Ars Technica hackers managed to crack 90% of 16,449 hashed passwords**
- **Six passwords were cracked each minute including 16-character versions such as 'qeadzcwrsfxv1331'**

By Victoria Woollaston Published: 12:17 EST, 28 May 2013

A team of hackers has managed to crack more than 14,800 supposedly random passwords - from a list of 16,449 - as part of a hacking experiment for a technology website.

The success rate for each hacker ranged from 62% to 90%, and the hacker who cracked 90% of hashed passwords did so in less than an hour using a computer cluster.

The hackers also managed to crack 16-character passwords including 'qeadzcwrsfxv1331'.

A team of hackers have managed to crack more than 14,800 cryptographically hashed passwords - from a list of 16,449 - as part of a hacking experiment for tech website Ars Technica. The success rate for each hacker ranged from 62% to 90%, including 16-character passwords with a mix of numbers and letters. The hacker who cracked 90% of hashed passwords did so in less than an hour

The hackers, working for the website **Ars Technica**, have now published how they cracked the codes and the traditional methods used to create an anatomy of a hack.

Rather than repeatedly entering passwords into a website, the hackers used a list of hashed passwords they managed to get online.

Hashing takes each user's plain text password and runs it through a one-way mathematical function.

This creates a unique string of numbers and letters called the hash.

Hashing makes it difficult for an attacker to move from hash back to password and it lets sites keep a list of hashes, rather than storing them insecurely as plain-text passwords.

This means if a list is stolen, the plain text passwords can't be obtained easily.

However, this experiment shows this doesn't mean its impossible.

When a user types a password into an online form or service, the system hashes the entered word and checks it against the user's stored, pre-hashed password.

When the two hashes match, the user is allowed entry to their account.

And using characters, a mix of lower and upper case letters and numbers creates slight variations of a hash.

The example, Ars Technica use is: hashing the password 'arstechnica' produced the hash c915e95033e8c69ada58eb784a98b2ed.

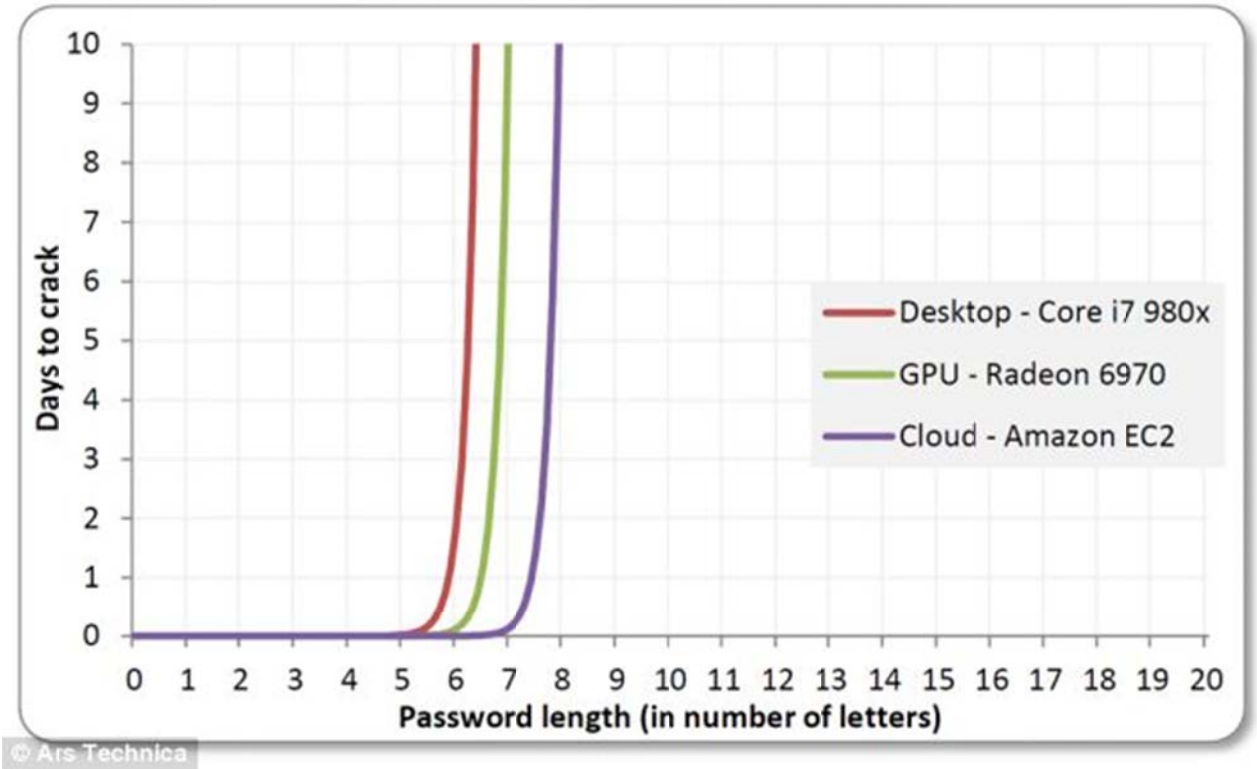
Adding capital letters to make 'ArsTechnica' becomes 1d9a3f8172b01328de5acba20563408e after hashing.

Jeremi Gosney, the founder and CEO of Stricture Consulting Group, managed to crack the first 10,233 hashes, or 62 percent of the leaked list, in 16 minutes.

It took Gosney just two minutes and 32 seconds to complete the first round, which found 1,316 plain-text passwords.

Gosney then used brute-force to crack all passwords seven or eight characters long that only contained lower letters. This yielded 1,618 passwords.

He repeated this for seven and eight-letter passwords using only upper-case letters to reveal another 708 passwords.



This graph shows how long in days it took the Ars Technica hackers to crack the list of 16,449 hashed passwords based on the method used. It also shows how long it took to crack passwords based on how long they were. Each hacker used a combination of wordlists, brute-force attacks and Markov chains to crack the list. One hacker managed to crack 90% of the list

Using passwords that contained only numbers, from one to 12 digits long, Gosney managed to brute-force 312 passwords in three minutes and 21 seconds.

Gosney has spent years perfecting word lists that contain a list of all the six-letter words, for example, to make cracking the weaker passwords faster.

One hurdle Gosney had to jump during stage one of the hack was 'salted hashes', a technique where sites add random characters to passwords to make them harder to crack.

This can include adding random numbers, characters or letters to the start or end of a password during the hashing process so hackers can't automatically enter a six-letter word, for example, and match the hash automatically.

However, Gosney explained that once one weak, 'cryptographically salted' hashes are cracked it becomes easier to work out the rest.

Once Gosney had obtained the weaker passwords, even those that had been salted, using brute-force he moved onto stage two.

Using a hybrid attack - which combines a dictionary attack with a brute-force attack - he added all possible two-character strings of both numbers and symbols to the end of each word in his dictionary.

Jeremi Gosney used a mixture of brute-force attacks, a hybrid attack that combined wordlists with brute-force attempts, statistically generated guesses using Markov chains, and other rules to turn a list of hashed passwords into plain text. It took him 14 hours and 59 minutes to complete all stages

He recovered 585 plain passwords in 11 minutes and 25 seconds.

He next added all possible three-character strings to get another 527 hashes in 58 minutes to complete.

Thirdly, he added all four-digit number strings and he took 25 minutes to recover 435 passwords.

In round four he added all possible strings containing three lower-case letters and numbers and got 451 more passwords.

In five hours and 12 minutes he managed to get 2,702 passwords.

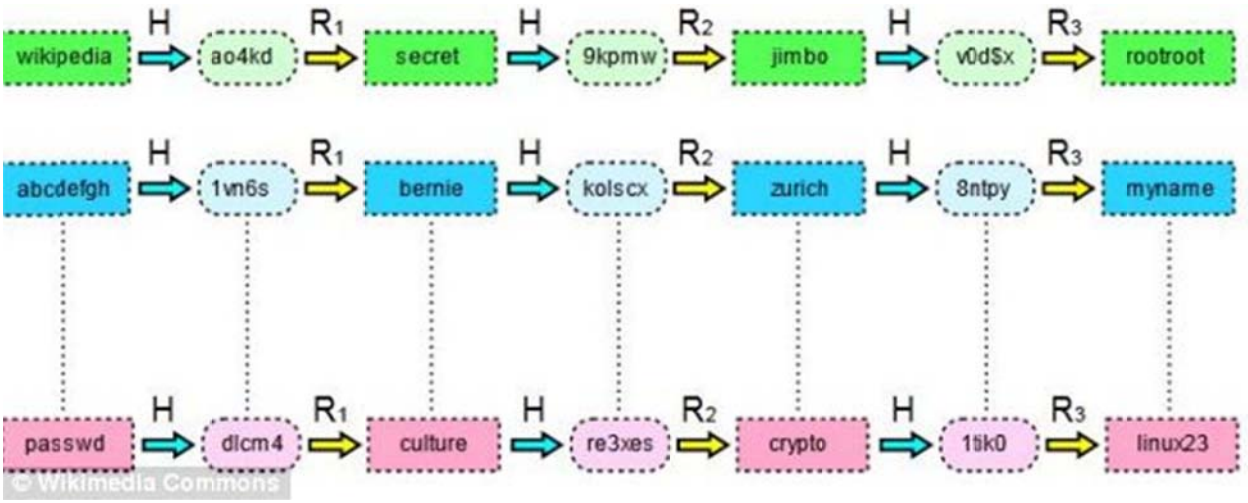
He continued to crack the rest of the passwords using a hybrid attack and cracked a total of 12,935 hashes, or 78.6 percent of the list, in five hours and 28 minutes.

During the third stage, in which Gosney attempted to crack the most complicated passwords, he used a mathematical system known as Markov chains.

This method uses previously cracked passwords and a statistically generated brute-force attack that makes educated guesses to analyse plain text passwords, and determine where certain types of characters are likely to appear in a password.

A Markov attack on a seven-letter password has a threshold of 65 tries; using the 65 most likely characters for each position.

And because passwords usually have capital letters at the start, lower-case letters in the middle, and symbols and numbers at the end, Markov attacks can crack almost as many passwords as a straight brute-force.



Hackers use a mix of wordlists, rainbow tables (pictured) and an algorithm called a Markov chains, among other techniques, to crack passwords from a hashed list. A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering the plaintext password, up to a certain length consisting of a limited set of characters

TYPES OF PASSWORDS RECOVERED

Some of the longer, stronger and more noticeable passwords that the hackers were able to recover included:

k1araj0hns0n

Sh1a-labe0uf

Apr!l221973

Qbesancon321

DG091101%

@Yourmom69

ilovetofunot

windermere2313

tmdmmj17 and

BandGeek2014

all of the lights

i hate hackers

allineedislove

ilovemySister31,

iloveyousomuch

Philippians4:13

Philippians4:6-7 and

qeadzcwrsfxv1331

From this method, Gosney discovered that people who don't know each other use very similar, and in some cases, identical passwords for the same sites.

During this third stage, Gosney also used other wordlists and rules and it took Gosney 14 hours and 59 minutes to complete all stages.

He managed to get another 1,699 more passwords - three hours to cover the first 962 plain passwords in this stage and 12 hours to get the remaining 737.

The other two password experts who cracked this list used many of the same techniques and methods, although not in the same sequence and with different tools.

They used a wordlist that was created directly from the 2009 breach of online games service RockYou.

This hack leaked more than 14 million unique passwords in plain text and this list is the largest list of 'real-world passwords ever to be made public.'

This method cracked 4,900 of the passwords. The same list was then used again, but this time the last four letters of each word were replaced with four digits. This yielded 2,136 passcodes.

Hacker radix then tried brute-forcing all numbers, starting with a single digit, then two digits, then three digits, and so, and managed to recover 259 additional passwords.

He then ran the 7,295 plain text passwords he'd recovered through the Password Analysis and Cracking Toolkit, developed by password expert Peter Kacherginsky, to identify patterns.

A 25-computer cluster that can cracks passwords by making 350 billion guesses per second. It was unveiled in December 2012 by Jeremi Gosney, the founder and CEO of Stricture Consulting Group. It can try every possible Windows passcode in the typical enterprise in less than six hours to get plain-text passwords from lists of hashed passwords

Radix then used this information to run a mask attack, which uses the same methods as Gosney's hyrbid attack but took less time.

He replaced common letters with numbers, for example he replaced 'e' with the '3' and recovered 1,940 passwords.

In December, Gosney created a 25-computer cluster that can make 350 billion guesses a second.

In an email to Ars Technica, Gosney explained: 'Normally I start by brute-forcing all characters from length one to length six because even on a single GPU, this attack completes nearly instantly with fast hashes.

'And because I can brute-force this really quickly, I have all of my wordlists filtered to only include words that are at least six chars long.

'This helps to save disk space and also speeds up wordlist-based attacks.

'Same thing with digits. I can just brute-force numerical passwords very quickly, so there are no digits in any of my wordlists.

'Then I go straight to my wordlists + best64.rule since those are the most probable patterns, and larger rule sets take much longer to run.

'Our goal is to find the most plains in the least amount of time, so we want to find as much low-hanging fruit as possible first.'

HACKING JARGON EXPLAINED

Markov chains - This method uses previously cracked passwords and a statistically generated brute-force attack that makes educated guesses to analyse plains and determine where certain types of characters are likely to appear in a password. A Markov attack on a seven-letter password has a threshold of 65 tries; using the 65 most likely characters for each position.

And because passwords usually have capital letters at the start, lower-case letters in the middle, and symbols and numbers at the end, Markov attacks can crack almost as many passwords as a straight brute-force.

Brute-force attack - Brute force also known as brute force cracking is a trial-and-error method used by to get plain-text passwords from encrypted data. Just as a criminal might break into, or 'crack' a safe by trying many possible combinations, a brute-force cracking attempt goes through all possible combinations of characters in sequence. In a six-letter attack, the hacker will start at 'a' and end at '//////'