passwords and security over a coffee

Business Services

orange™

editorial

Passwords are everywhere: in your computer, your webmail or your online bank account. Everyone knows they must be strong but we always try to simplify them as much as possible: there are so many passwords in our lives that you just can't remember them all. So we all have our own tips and tricks to cope with this: we use the same passwords over and over again, we write them down or we even use the dog's name or the date of birth of our latest child. This is a nightmare for us all.

All this allowed us to write a numerous amount of blog posts around this nightmare and you guys helped us a lot. So thank you for that! These blog posts will make things clearer so that you understand how sensitive these characters can be.

Enjoy,

Sébastien Roncin

content

passwords: the key to keeping your secrets locked up tight

by Sébastien Roncin

The topic of the day is passwords. We say all the time that you have to change your password regularly. And that you need a strong password. But what does that mean? And why?
How can someone crack a password?

cracking a password

There are three ways to crack a password: brute force, dictionary attacks and social engineering (in the IT sense, not in the political sense) .

Brute force is the easiest way to crack a password. It always yields a result if you have enough time on your hands (a lot of time in many cases). The technique is to simply try every possible password combination until you find the right one.

Dictionary attacks require a set, or "dictionary," of possible passwords. In this method, you try all the words in the dictionary until you find the right combination. Obviously, if the right combination isn't in the dictionary, you can't crack the password. However, these dictionaries are compiled from a set of common passwords. So statistically speaking, you have a high chance of cracking most users' passwords.

Lastly, **social engineering** consists in sending a survey to users to obtain information about their life, family and other interests so as to find new password possibilities.

Some of you are probably rolling your eyes and want to tell me that websites only allow a certain number of password attempts. So it's difficult to crack a password. But you also have to remember that passwords are generally stored on the computer used to enter them. Fortunately, passwords are not easily found but they do leave a trace. You just have to try every possible password combination until you find the right trace.

change your password regularly

The more you change your password, the more you limit the risk of your password being used if it's cracked and the more an attacker will have to redo the search process. **This is the idea behind so-called strong logins**, where you are assigned a "random" password. The more you reset the password, the less time attackers will have to crack it (for strong logins) and the lesser the chance they will have to use this password.

But always try to avoid one of the most common pitfalls: since people have to change their passwords so often, they tend to make them weaker to more easily remember them.

good to know

A good password has upper and lowercase letters, numbers, punctuation marks and any other characters on your keyboard.

betting on strong passwords

Most people's passwords only use the 26 letters of the alphabet. I won't spend a lot of time on the different kinds of predictable passwords:

- kid's names
- pet's names
- "qwerty"
- "password"

as well as short passwords because we're usually pretty lazy when it comes to logins.

Today, the average password is only eight characters long. These passwords create 200 billion possible combinations. Since the average computer can run about 100 billion operations per second (with graphics capabilities, computers can sometimes reach more than two trillion operations per second), almost anyone's computer can crack these passwords in about one second using brute force. That time is even shorter when using stronger calculation tools.

What happens if you use **both upper and lowercase** letters? The number of possible combinations will grow from 200 billion to 50 trillion. Now an attacker will need a lot more time to crack this password: a little over four minutes.

Basically, the more characters you use, the stronger your password becomes. That's why you should always **add more characters to your passwords**:

- upper and lowercase letters
- numbers
- punctuation marks
- and any other characters on your keyboard.

When you use all the different types of characters available (approximately 90 characters in all), you expand the pool of possible combinations to four million billion. That means more than six hours of constant calculation to crack your password!

how to evaluate a password's strength?

Six hours may seem like a lot but it's still relatively fast. It's even faster if you use more powerful calculation tools, like the power offered by cloud computing providers and botnets.

Since characters are limited, you have **to use size to create even stronger passwords**. With each extra character, you multiply the number of possible combinations by 100 which adds over 22 days to the time needed to crack the password. With this kind of password, attackers will really have to want to crack it. With each extra character, the process becomes exponentially more difficult.

The table below shows the total number of possible combinations for each password length. I also added the time needed for one of the biggest botnets ever created (Rustock, which was made up of about one million computers) to test every possible password combination (a calculation power that has yet to be equaled by any supercomputer or network, such as Folding@home).

For comparison, remember that the Earth is only about 4.5 billion years old and the universe is about 13.7 billion years old. That's less than the time needed to crack a password with 18 characters using current computing power.

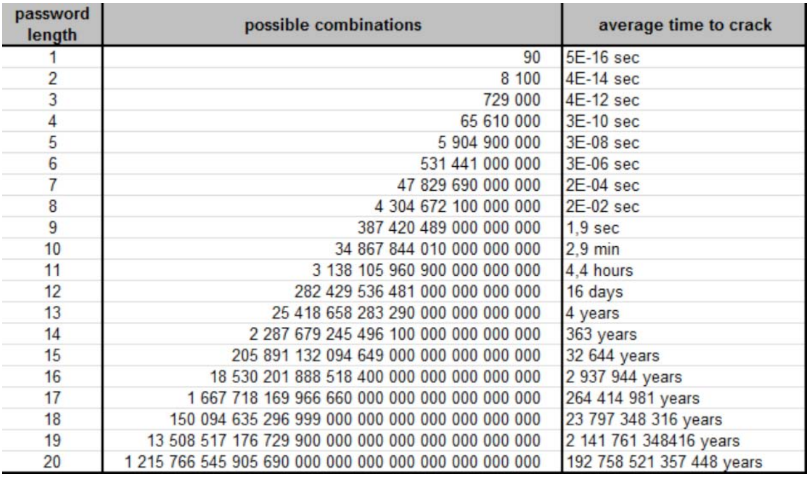
It's scary that most websites recommend passwords of at least eight or nine characters. It also goes to show the quality of advice on a lot of websites!

> "average global computing power climbs by a factor of 10 about every four years"

warning

If your password has over 13 characters, you can assume it will be nearly uncrackable.

good passwords



password length	possible combinations	average time to crack
1	90	5E-16 sec
2	8 100	4E-14 sec
3	729 000	4E-12 sec
4	65 610 000	3E-10 sec
5	5 904 900 000	3E-08 sec
6	531 441 000 000	3E-06 sec
7	47 829 690 000 000	2E-04 sec
8	4 304 672 100 000 000	2E-02 sec
9	387 420 489 000 000 000	1,9 sec
10	34 867 844 010 000 000 000	2,9 min
11	3 138 105 960 900 000 000 000	4,4 hours
12	282 429 536 481 000 000 000 000	16 days
13	25 418 658 283 290 000 000 000 000	4 years
14	2 287 679 245 496 100 000 000 000 000	363 years
15	205 891 132 094 649 000 000 000 000 000	32 644 years
16	18 530 201 888 518 400 000 000 000 000 000	2 937 944 years
17	1 667 718 169 966 660 000 000 000 000 000 000	264 414 981 years
18	150 094 635 296 999 000 000 000 000 000 000 000	23 797 348 316 years
19	13 508 517 176 729 900 000 000 000 000 000 000 000	2 141 761 348416 years
20	1 215 766 545 905 690 000 000 000 000 000 000 000 000	192 758 521 357 448 years

To summarize, a good password uses **every character type available on your keyboard**, does not contain any word in any language or any names, and is **at least 13 characters long**. For now!

Yep, that only goes for now because computing power is growing exponentially. Average global computing power climbs by a factor of 10 about every four years. This means that in four years, we can assume that the biggest botnet available will have multiplied its power by the same factor. So the 13-character password that we recommend today will have to add another character to remain uncrackable.

Considering how long a strong password has to be, we're really going to have to either improve our memories or come up with something a little more clever . We say password, but nothing says you have to use just one word. You can always make a passphrase based on **a sentence you'll remember**.

For example, you'll always remember your kid's academic milestones with the phrase "**Tom graduated in 2012.**" Then you just use whatever method you like to blur the sentence a little: "T0mgr@duat3d1n2012." That's 19 characters, a nice variety of character types, and there's no chance your password will be in any dictionary on Earth. So you can rest assured until you need another password.

original article
http://oran.ge/W7xUBO

the great password masquerade

by Jean-François Audenard

People who work in IT security (including me) often defend old habits that should really no longer be in use. Passwords are one of the places where a few different 'obsessions' have remained deeply rooted for years. And the three 'golden rules' put forth for passwords are generally:

1. change passwords regularly
2. create complex passwords
3. choose different words for each website (don't reuse the same word)

But the reality is that users rarely if ever follow these rules: either these **rules are no good**, or users simply don't understand them. Right off the bat, I would go with the first answer. This is what this article is about, which I have aptly titled "the great password masquerade."

So if you're ready, then let's get started!

a right hook to rule #1

Forcing users to **change** their **passwords regularly** (every 6 months or so) just encourages them to use strategies like "OK I'll just turn this 8 into a 9." This is completely pointless. Let's take an example:

- before: SuPe5Passw@rd!
- after: SuPe6Passw@rd!
- or even: $uPe5Pass@rd!!

This is an easy enough way to pacify any system that makes sure passwords are sufficiently complex (see rule #2). And all is good for users, since they will always be able to remember their "new" passwords. But the problem is that passwords become very predictable this way. Even worse is that substituting a $ for an S or 0 for an o is useless: any decent crack tool already knows that trick.

In fact, **the threat is no longer posed by brute-force attacks** but rather by phishing and other keylogging attacks. So rule #1 is obsolete and needs an update. At the same time, rule #1 also clearly doesn't jive with rule #2, which says that passwords should be complex: users will always forget new, complex passwords.

The only real reason to change your password: if you think (or suspect) that it has been compromised. So you really just have to keep an eye out for these kinds of problems. See my thoughts on rule #3 for more on this topic.

bam! rule #2 takes a jab to the face

Sure, **complex passwords** can be cute with their lowercase and uppercase letters, numbers, and special characters, all (of course) adding up to 6 or 8 characters or even more. Obviously, these are **a challenge to enter**, especially when using a **tablet or smartphone**. These devices just weren't made for these kinds of finger gymnastics.

Of course, you can't just use words from the dictionary or tricks like qwertyuiop or any other worthless passwords like 1234567890. Since the goal is to avoid things that are too simple, it's best to use long passwords of 25 characters or more:

- mypasswordiscaptainhook
- strawberryisthebesticecreamflavor

Websites that limit passwords to 8 characters are weak. This is a telltale sign that they store passwords with no encryption (yep, because MD5/SHA1 hash codes are the same size no matter the password).

rule #3 is the lone exception

Using the same password for every website is just careless. It's best to have **a different password for each website**: that's what I do (yep, I'm a bit obsessive; just ask my wife). What does this strategy look like? Well, I have something like 136 different passwords in all. And don't forget your little notebooks and **password managers**.

For those of you who still have some sense of sanity left, it's a good idea to **pool your passwords**: 4 or 5 passwords for 4 or 5 different website groups (one for all news websites that do not use any personal data,

good to know

Using the same password for every website is just careless.

another for websites that collect some sensitive data, etc.), and one special password for all sensitive websites.

conclusion

So maybe I'm going a bit against the grain here: it just might happen that a price will be put on my head and hundreds of agents from the CIA, FBI, and the NSA will be waiting for me outside the office. It's true that I'm challenging the system a little, but isn't security there to be challenged?

We need to throw out our antiquated rules, because that's the only way to make progress! So chuck rules #1 and #2 in the garbage, but be sure to keep rule #3 in a safe place!

original article
http://oran.ge/16aKFzN

how do you evaluate a password's strength?

by Vincent Maurin

Many password generation tools are available in the form of user interfaces and libraries for developers.

However, the increasing number of passwords (for system sessions, inboxes, web interfaces, e-commerce sites, social networks, etc.) does not allow account managers to implement a policy that generates passwords for users.

The current (quite natural) trend is to enable users to define their own passwords while imposing a certain number of requirements to ensure password strength (using at least one capital letter, one special character, one number, etc.).

How should a password strength policy be created? Below are four online tools to help everyone approach this topic in a fun, educational way.

how secure is my password?

The website howsecureismypassword.net attempts to answer the question in simple, layman's terms. It shows users how long a machine (powerful enough to analyze 10 million combinations per second) would take to break a given password.

- informative value: low
- layman's value: high
- target audience: uninformed users
- comments: giving a specific time period helps the tool raise awareness

Microsoft Password Checker

The Password Checker tool in Microsoft's PC security section is not on par with what the software giant could offer.

- informative value: low
- layman's value: low
- target audience: uninformed users (those unfamiliar with security)
- comments: the primary colors make it look like a game for kids

Password Meter

Much more elaborate than the two previous tools, Password Meter explains the criteria it uses to assess password strength. It gives your password a grade of "Failure", "Warning", "Sufficient" or "Exceptional" in each of its categories.

- informative value: high
- layman's value: average
- target audience: people who want to learn more about password strength criteria
- comments: though unattractive at first glance, the tool is highly informative

Password Strength Test

In the same vein, Password Strength Test has a pared-down look but provides a wealth of important information. It succinctly outlines the metrics used to generate the final grade (character set size, entropy). An accompanying text explains which contexts are appropriate for the password and how users can improve their score, if desired.

- informative value: average
- layman's value: average
- target audience: people who want to learn more about password strength criteria
- comments: the tool's visually austere display will not encourage use

additional notes

The technologies used by these kinds of websites rely on JavaScript. As a general rule, no data is transmitted to the server, which limits the risk of attackers hiding behind the tool's host website. Nevertheless, **using your real password is not recommended**. It's better to use a variation that moves or reverses certain characters, for example.

original article
http://oran.ge/10jLkOV

about the authors

Jean-François Audenard

Within Orange Business Services, I'm in charge of securing our cloud computing solutions and services. I'm the passionate kind and only look at things this way: no 50/50 for me, I'm an engaged and engaging blogger, I like to go off the beaten track. Sincerity is my tone and optimism and voluntarism my two engines.

Vincent Maurin

I work for Orange Business Services as a security leader within Products and Services Development. My previous jobs as a technical "worker bee" lead me to pay specific attention to the difficulties of implementing companies' security strategies and policies. Security, efficiency and pragmatism are my main pillars.

Sébastien Roncin

I don't know anything about security: I'm in marketing and I'm a security product manager since 2009. My goal: popularize security and teach the average Joe about risks and their solutions.

our blog:
http://www.orange-business.com/en/blogs/connecting-technology

document available for download at:
http://www.orange-business.com/en/library

Edited by Orange Business Services
08.03.2012

France Télécom – 78, rue Olivier de Serres, 75015 Paris, France – SA au capital de 10 595 541 532 – 380 129 866 RCS Paris – Document non contractuel – juin 2012

Business
Services

orange™