Extended Definition: 'Password Safety'

Daman Morris

In this extended definition, I will explore the concept of "password safety" from the perspective of the Electronic Frontier Foundation (hereafter, EFF). According to their website, the EFF is an organization that "[defends] digital privacy, free speech, and innovation". As part of this goal, particularly as part of defending digital privacy, the EFF would have a natural interest in informing consumers about password safety. To that end the natural audience for this extended definition consists of consumers who make use of any digital product secured by a password. The audience is thus quite diverse, as the products used range from simple email clients to industrial-level software used in a work environment, potentially handling sensitive and confidential information. In addition, it cannot be assumed that the audience in general knows anything about digital security or password safety in particular, or even that they are particularly "computer literate". Thus, this extended definition will cover the basics of password safety and basic computing security terminology intended for a general audience of personal computer users. It would be most suited to appear as an article or blog post.

Passwords are a simple but widely used form of digital security. A password consists of a string of letters, numbers, and special characters. Some vendors choose to limit the use of certain characters as a naïve form of **sanitization**, which is a more general process that attempts to prevent malicious entities from exploiting internal details of a system and gain unauthorized access (the details of such exploitation are outside the scope of this document, but one example of a potential attack taking advantage of poor sanitization is SQL injection). More sophisticated sanitization procedures exist which allow the use of special characters, but these are more complicated to implement, so vendors may differ in the set of characters allowed for a password. Generally, the allowed character set will be explicitly presented to the user when choosing a password. Passwords provide security by making it theoretically impossible for an unauthorized user to gain access without knowing the password. However, a password is useless if the malicious entity can reconstruct or steal the password. Thus, a critical part of password safety, ignored by many people, is to protect oneself against so-called **social engineering** attacks. In a social engineering attack, a malicious actor pretends to be an official or authority of some sort and tries to get the holder of a password to answer questions that would allow them to either guess the password or manually reset the password through the vendor's password reset functionality, using the answers provided by the password holder (e.g., "what is your mother's maiden name?", "what street did you grow up on?", "what was the name of your first pet?", etc.)

Assuming that the attacker knows nothing in principle about the password, their last option is to guess the password by **brute force**. A brute force attack consists of listing all possible passwords in the **password space** and trying them one by one, where the password space is simply all possible passwords. Because the password space is finite, it is theoretically possible for an attacker to arrive at a correct password by "guess and check". However, whether this is *feasible* or not depends on the size of the password space. For example, if a password is only one character, then a conservative upper bound on the size of the password space is around 100 passwords (depending on how many characters are allowed in passwords). Any modern computer can try 100 passwords in a fraction of a second, meaning that a one-character password can easily be guessed. For a two-character password, the number of possible characters is squared, so there are 10,000 possibilities. This may seem large, but it is still child's play for any modern computer. Experts disagree about the precise minimum bound for a "safe" password, but generally passwords of between 16 and 20 characters are considered safe for most purposes.

Finally, there is the issue of passwords being duplicated between different services. Many people have one password for several or even all of the online and offline services they use. However, this is highly insecure:

if, for example, one of the companies you use a password for has a **data breach**, wherein the passwords of some or all of their customers are publicly leaked, a savvy hacker can (and will) simply take all those passwords and try them on as many sites as they can find. In the worst case, if you use the same password for everything, even one data breach for one service you use can allow a malicious actor access to *all* of your online data. Thus, one of the best ways to secure yourself against hacking is simply to use different passwords for each different service. One particularly effective way to do this is to use a **password manager**, which is a program that stores all your passwords on your local computer (which, presumably, no malicious actor has access to) under a single password, combining the convenience of having a single, memorable password with the security of having different passwords for everything (which need not be memorable since the program "remembers" them for you).