Security by password authentication – do you remember them all?

It is a well known fact that human brains are not designed for remembering numerous long and complex infrequently used phrases, a.k.a passwords. However, despite all recommendations from a security usability point of view, most of the applications were built depending on a human memorable password. Even nowadays it remains being the key authentication system for most applications and services. Could it be possible to create an even bigger design flaw in something that is supposed to be completely reliable and secure?

First of all, let's examine the very simple notion of a basic password that each of us must have to access any protected digital entity. How secure do you think is your password? Did you ever really try to test it against a password cracking tool to verify that it doesn't fall in the category of weak and easily crackable passwords (not just following up the indication provided directly to you highlighting how secure or not is your password)? If you never did, give it a try right away. Take for instance one of the most popular ones password crackers, John the Ripper. Give it a shot first with the password for your system. No luck? Good! Probably it is secure enough to be resistant against basic cracking tools. But what if you will try it now with the password that you usually use for some silly websites, which so desperately need to create an account for you with a password? AHA! Seems that this time there is more luck! And yes, it is quite normal, as we are all just humans. We tend to choose something really short and simplistic for things we don't care... But there is always BUT! Did it ever happen to you to reuse that same password on other sites, important and not important? To make matters worse, over time you start to be confused if this site ever was and still is useful or not. And here it comes! The main problem of the password-based authentications. Imagine if one of such silly websites got compromised (or even not compromised, just by a sheer lack of security the password got sent back to you in clear text as a confirmation of your account creation), and here you go – potentially your password that you used on many other sites got added to database of "crackable" passwords...

What about a better approach? To avoid memorising different complicated passwords for every single new web site, just use a password manager. There are many available in the wild: browsers extensions, plugins, apps on a client side... Did you ever try any of them. For example there are LastPass, KeePass, 1Password, Firefox's Password Manager, Chrome Account Manager. While it is true that the use of these tools brings several security related improvements, such as secured storage (no need to remember) and key generation (complexity and entropy increase), it still has flaws raising the questions on usability and trust.

Another devil follower of the password problematic is called "Open data passwords", or better known as "Security questions". Thankfully, more and more systems are abandoning this old way of providing additional security! However, even the most popular webmail providers still have to deal with the legacy "leftovers" to restore access to lost accounts and this seems to be really problematic with no good solution still available.

As password security is the main topic here, it is important to mention one of the side effects of password authentication, namely theft of your credentials. If there would be no passwords – there would be no phishing, as impersonating a website or email to steal your passwords are the most common approaches for phishing. To alleviate this problem and to reduce the risk of becoming a phishing victim, there are some really nice solutions to look into.

Browsers built-in security: ensuring that the password stored for website matches the domain name.

Two factor authentication: several combinations exist for unlocking protected assets, e.g. phone app using code generator, phone app using QR code, card reader, USB dongle.

Trusted Computing: the computer hardware is expected to behave in a particular way, enforced by hardware embedded software and/or operational software at a higher level.

In GHOST project, the end user is given a central role. The end user behaviour and

aptitude is integrated into security solution right from the beginning of the system design, allowing to build a system where human flaws are known and timely addressed. This is why GHOST doesn't rely on a traditional password-based authentication. Instead, a blockchain enhanced authorisation system is put in place where only GHOST registered users can control and monitor their smarthome.

Document History

#	Date	Description
0.1	30/03/2021	Original version for GHOST project
0.2	30/03/2021	Republished for I-Sec website

The Information Security Group

UNIVERSITÉ
DE GENÈVE

Geneva School of Economics and Management
Information Science Institute