INTROSEC HT2020

Problem 1

Passwords are still often used. Name and explain security problems when relying on passwords, and problems when people have to use passwords (considering the following two scenarios). Explain how to mitigate the problems caused by passwords and whether the mitigations will introduce other problems (Note that the mitigations are not limited to using passwords).

a) A bank where you log in with your Swedish ID ("social security number") and a password you chose yourself.

b) A web-page where you can check your mobile phone surf usage/balance, and perform simple tasks, that comes with a password generated by the provider. This password cannot be changed by the user.

Solution

Passwords are a security measure that is widely used nowdays. Along with it's positives it also brings negatives.

Lets take a look at both of the above senarios seperately.

a) The social security number is something that may not be known to many people but still can get out there. And it is also not hard by someone to find it. It is something that is in a conspet public. We also have a password in this case combined with the social security number to log in. So the social security number provides the identification and the password provides the authentication. It is easier for someone to know your identifier, it is public. So someone can get access to you Swedish ID. The password is private. There are issues with it too though. It can be stolen by someone or can be easily forgoten. Most password people use are also not that large cause it is hard to remember big passwords and usually people choose something that they may associate with for example their birthday. There are online dictionaries that can be used to crack passwords especially when they are not that big. With the computational power we have nowdays using bruteforce can lead into cracking those passwords.

The solutions that can be offered in this case include users to change passwrods very often. For example some banks have the user change passwords every 6 months and they cannot use any password from the past. Also the users could be made to have passwords larger than a specific number of characters. That could make passwords more secure and harder to crack but it could increase the factor of the password being forgoten. Another solution in terms of the identifier

is too actually create it in paires. What does that mean though? Well, the user could have the Swedish ID to use it for example when he goes in the bank in person. When he is trying to log in on the webiste of the bank and do activities online he could use another identifier less known that is in pair with the Swedish ID. That of course doesn't mean that that number will not be found, but it may be harder.

b) Let's start with the mobile number. So many people have access to it. So it for sure is widely known and not private. You give your phone number to many companies, frinds etc. Also sometines numbers cab be found in phone books. So in this case the password should really be strong. It can of course be stolen or forgoten. The fact that it is also a password assigned by the company may make it harder for people to remember since they are random passwords not assoicated with something particular. That may lead to them to save it on their pocket for example or in folder in their laptop. Very easy to find them. Also in this case since the passwrod cannot be changed, if someone finds it in someway they have access forever and you may not even realise it.
One solution here is for the company to apply another policy in terms of the passwords, that could be the passwords to be changed by the company for example every three months. That tough could be incovinient since the user will face issues as learing and remebering passwords very often. That is not the best user experience.

When it comes to mitigations of the problems caused by the passwords in both cases we could use passwrods saving software such as KeyPass and LassPass. There you could save every password of yours and that software is proven to be much more secure and used widely. The danger that you have to take here is that if someone find your passwrd to that software then you loose all the passwirds together. Another solution is to use biometrics combined with passwords. If you want something even more secure don't have the user to use only password or only fingerprint but also both of them combined. The issue with biometrics is that they can be forget or in some cases some people do not have them. But combination of both of those make for better security. Last but not least we should teach users about good password policy and the importnace of it.