The Riddle of On-Line Authentication

Abstract

Password authentication is as old as IT is, and it has always been known to carry many security risks. With the advent of internet and on-line services, the use of passwords has exploded becoming one of the weakest points of our daily internet experience. A lot has been tried to improve the authentication process, but every day we still deal with too many passwords. In this article we review some of the most important issues related to on-line authentication and the never-ending life of passwords.

Authentication to IT devices, computers, portables, tablets, smartphones etc., has always been a complex, annoying, difficult and risky issue. Since before the era of networking, those working with computers had an account on each machine, often with different usernames since they were chosen by the system or the system-manager. The user had to choose a password, and more often than not, people tried to use the same password on different systems just to make it easier for themselves.

With the advent of networking, the possibility of choosing not only the password but also the username, and the exponential growth of the number of accounts a single person has to manage, it has become quite diffuse the trend of using the same username+password combination at least every time possible.

It is a handy habit, but quite disastrous from a security point of view.

Even if for more than 30 years (and in computer years this accounts for many generations and eras) username+password has been known as a security problem, no final solution has been found to the security of the authentication problem, which is particularly important for on-line authentication.

In this short article we review at a not too technical level, what is the current situation on the problem of authentication, in particular on-line, starting by looking at the most obvious approaches that can and have been taken to tackle it.

The On-Line Authentication Issue

As of today, any person using on-line services must register to web-sites, applications etc. This means that every person, and for each service, has to create a valid set of credentials that identify and can be used to authenticate precisely, securely and individually him or her.

Here lies the first problem:

one person <= versus => many credentials.

In an ideal world, to identify and authenticate one person it should be possible to have one set of credentials that can be used for any IT application, device etc.

Indeed this is what (almost) happens (or happened) in the physical life: each person has one passport which is the person's credential. But then we also have a driving license, a national identity card, a social security card, cards for all kind of shops, offices etc. So the “one person vs. many credentials” issue is not only for our digital life, but also for our everyday physical life.

It is generally believed that authentication mechanisms can be organized in the following three categories:

- knowledge: something one *knows*;
- possession: something one *has*;
- inherence: something one *is*.

The main difference between the physical case of passports, cards etc. and the username+password authentication mechanism is that the first is mainly a possession mechanism, the latter a knowledge mechanism. We can have 50 cards in our purse, but it is more difficult to remember 50 passwords, unless of course they are all equal or we write them down on a piece of paper.

Biometrics

A few years ago many thought that biometrics, that is using biological characteristics of the human body like the fingerprint, would have been the final solution to the authentication problem. Notice that biometrics belongs to the inherence category of authentication mechanisms.

It has not worked out as expected and probably it never will. Some of the reasons for this are technological but other are intrinsic to the biometric approach like the following [2]:[1]

- Privacy: biometric characteristics of a human being are unique and intrinsics to its being, at least in Europe there is a lot of concern about the privacy consequences of their widespread use;
- Un-replaceability: suppose that some biometric credentials are lost, stolen or duplicated, by their definition they cannot be changed, so a person would remain without credentials and a thief could fully impersonate the original person; there is no mechanism like a "change of password" for fingerprints;
- Security: most biometric devices have shown weaknesses and proneness to false positives, that is accept as true false, copied or imitated credentials, and also to false negatives, that is to reject true credentials; other security issues are the protection of the databases of biometric data and the security of the protocols that would allow all kind of devices to provide authentication with respect to the biometric credentials;
- Cost: in principle one could imagine that a biometric authentication procedure should cost little, since it is based on the human body; on the other side the reader of the human body characteristic is quite a complex object which should be available on each device that requires to authenticate the person.

As it is now, biometric authentication is adopted for very special, limited and high security environments, where it provides the added security required by the situation.

---

1 "Behavioural biometrics", that is authentication based on the behaviour of a person and not on a biological characteristic, seems to offer another possible approach carrying less problems.

The passwords' problems

The most basic and still fundamental authentication method is the password. In theory passwords are very clever authentication mechanisms of the knowledge category, but they have many practical problems which make them difficult to manage by individuals [1]. Some of the main problems are:

- it should be difficult to guess a password both by someone that knows the person and by brute force trying many passwords with special computer programs; good, un-guessable passwords are so complicated, practically random, and long that they are impossible to remember, as it is required by their belonging to the knowledge category, that is something that only the person knows;
- each credential must have a different password, that is for each system, service and application one can use the same username but must use an unique, never used before and anywhere else, password; otherwise one falls in a kind of "all eggs in a basket" situation where the basket is the password and the eggs are all systems, services and applications that use that password; the risk is that if for any reason that password is divulged or guessed, all credentials using it are in principle lost;
- even if passwords are pseudo-random and unique for each credentials, they should be managed, for example changed periodically, and there should be procedures to recover or substitute them in case of loss.

One important point about passwords is that to work as knowledge authentication category, they must be never written down on any kind of support, digital or physical, otherwise they change category and belong to the possession authentication category. The difference could seem small, but it isn't: once a password is written down, its support becomes its main protection and if the support with the password on it is stolen or lost, also the password is lost, even if one still remembers it by heart.

Managing Passwords: Wallets et al.

In theory, and in part also in practice, it is possible to manage the passwords in a reasonable secure way. Probably the method is not very comfortable, but one can get used to it. What one should do is:

- generate a secure (eg. sufficiently long) pseudo-random password for each credential;
- since it is obviously impossible to remember all such passwords by heart, store each credential with associated password in a secure way;
- have simple and secure procedures to recover the passwords and use them in the authentication procedures.

Most of this can be done by means of "Password Wallets" also called "Password Managers": these are applications that can

- generate pseudo-random passwords;
- store the passwords and the associated credentials;
- allow to retrieve, typically by copy-and-paste, the passwords or, for some applications, to perform directly the authentication and login procedure on behalf of the user.

The Password Wallets protect the password by encrypting them and the user can access the Wallet either with a password or with a token like a smart-card, a usb-token etc. In practice one can trade to remember many un-secure passwords for a single password used to access the Wallet.

Moreover, there are by now many on-line Password Wallet services that permit to store all passwords in a single on-line place and access them by multiple devices: PCs, smartphones, tablets etc.

Problems of the Password Wallets

Password Wallets are very good ideas, and the author of this article uses them, but they have their own problems.

The first problem is usability and diffusion: very few people use them, and unless something is done to force their adoption, it will probably remain that only a small number of risk-averse people will ever adopt them.

They also are another case of "all eggs in a basket" situation, where now the basket is the Wallet and the eggs are the passwords. Some risk scenarios in this case are the following:

- for a file-based Wallet, if the file is stolen and the Wallet password is not too strong, there is

a high risk that an attacker can open the Wallet and extract all credentials together with the associated passwords;

- the same risk applies to an on-line Wallet, if the Wallet password is not too strong or the Wallet service has a serious vulnerability that allows an attacker to extract the credentials from the service.[2]

Finally, the use of a Wallet slightly changes the knowledge category of the password authentication mechanism: the user knows the password of the Wallet, not the individual passwords stored in the Wallet, and if a token is used to access the Wallet then the full authentication category becomes possession, that is something one has. The individual passwords in any case belong to the authentication category possession, which means that they can be stolen or lost as objects as already mentioned.

Another risk which is not enough appreciated with Passwords Wallets is that when a Password Wallet is opened, then all processes with the same or higher privileges as the user, can access it. The simplest case is the presence of a virus on the user machine which can read all contents of the Password Wallet as soon as it is opened [3].

Password Wallets can be used in a larger number of situations and by a larger number of users than biometrics, still they do not solve the authentication problem.

Two Factor Authentication (2FA)

Since we have not been able to do without passwords, what has been done was to improve on password authentication. Since password authentication is of the knowledge category, one can add a second authentication to the same login of the possession category. This implies that to authenticate it is necessary to provide a username, a password and a third data which proves the possession of an object or a device.

Many different solutions have been proposed and implemented among which the more common are:

- a smart-card or a cryptographic usb-token which requires a smart-card reader and/or additional software to manage the connection and the authentication process;

---

2 This risk should not be underestimated due to the weaknesses of the security of current on-line IT technologies.

- a token which produces a pseudo-random key, typically a number, which changes often, at least a couple of times per minute, and that is used as a second password, that is typed-in the authentication screen of the application;
- a grid-card which is a printed card containing pseudo-random keys, typically numbers: the authentication process asks the user to type-in a specific key as a second password (usually the keys can be used only once, but they are not time-limited so they can be stolen or copied and used at a later time);
- a mobile phone to which the application sends an SMS or makes an automatic phone call providing the user with a pseudo-random key, typically a number, that is used as a second password.

The most important point is to use another physical device and communication channel for the authentication, not the one used for accessing the application.

In the first three examples above, the authentication device differs from the IT device, but on top of the cost and complexity issues to implement and manage such solutions, to access many different applications a person ends up having many different authentication devices to manage and keep.

The mobile phone seems to be an interesting solution, but the access to the application should not be done on the phone itself otherwise there will be no difference between the device which provides authentication and the device on which the authentication is done. In other words, it will not really be a 2 Factor Authentication.

Moreover, mobile phones are IT devices with reasonable large risk of being attacked and abused so to intercept the authentication keys. Indeed there have been already cases of malware intercepting SMS and data on smartphones to steal authentication keys [4].

Finally it should be noticed that mobile phones are becoming more and more little, but powerful, mobile computers and that all communication, including voice and SMS, are migrating to Internet Protocols (IPv4 and IPv6) so that using mobile phones for 2FA has a reduced value from the security point of view.

Summing up, using smart-cards and tokens for 2FA is currently one of the best approaches for applications with high security requirements. Costs and manageability make these solutions difficult to apply to large scale, medium and low security risk applications.

For large scale, medium and low security risk applications it seems ok to the use smartphones as a 2FA mechanism, with the exception of applications running on the smartphone itself.

Single Sign-On and "Login With ..."

Still users have too many accounts, passwords, 2FA mechanisms etc. One way to approach this problem is to allow users to access online applications once they have been authenticated by a "trusted" identity provider. Technically this is achieved by means of managing Federated Identities[3] between applications, that is sharing identities, and adopting Single Sign-On (SSO). In this way once a user is authenticated by one application, she/he can access also the federated applications with the same credentials and without need of authenticating her/himself again.

Most of the large internet companies provide Federation and SSO services to other applications, from Microsoft to Google, Facebook, Amazon, Yahoo!, Twitter, Linkedin etc.

If a user is logged in with one of these providers which is federated with another application, then to access the second application the user does not need to use any new credentials nor to go through a new authentication process. In theory it could even be possible to access any online resource just with a single credential and login.

Federation and SSO can make the life of internet users much simpler and more secure, but at the same time introduce new security risks.

The first risk is again of the "all eggs in a basket" kind,[4] where if someone manages to access the single credential used for SSO, to guess the password, or if there is a vulnerability in the Federation system, then all applications accessed with that credential are simultaneously at risk.

This is the reason why high security applications, like online banking, usually do not accept SSO login from other identity providers, and in case only act as providers of identity to lower security applications.

The second risk is about privacy: adopting SSO to access online resources, can make it easier to trace the online activities of a person, this just because the same credentials are used to access

---

3 Technically there is a difference between Federated identities and Delegated identities but it is not really important for what is discussed here.

4 More precisely, this is "one key to open all doors".

different applications.

Password reset

A final hurdle with managing credentials and passwords in particular, is the issue of "reset". It can seem trivial, but the mechanism to reset a password can become a very big security hole and be the starting point to break-in the accounts.

Unfortunately quite often people forget the password or just need to reset the password without accessing the account itself. Within a company this can be done efficiently and easily by physical means, that is going in person to the IT system manager and having the password reset. This can not work with large online services. Moreover the process should guarantee that nobody else than the user will know at any moment the password to access the account.

The current approach to online password reset is to have established a second channel of communication with the user, typically email but also a telephone.[5] The user then selects his own account name and either by clicking on a link or by asking an operator on the phone, has the password of the account reset and an information automatically sent to the second communication channel which allows the user to establish a new password. If email is used, in the email is provided a link which leads the user to a special page of the application where the user can insert the new password. If an SMS is used, the code sent in the SMS together with the new password allow the user to establish the new credentials.

At first sight this approach seems to work fine, but it has shown in the last years to be difficult to manage and to have various security risks, which have been exploited many times [5].

First of all, if email is used as a second channel, this method cannot be used to reset password for email accounts, otherwise the user will never receive the link to follow since it will be locked inside his email account by the password reset. So to perform a password reset for an email account, other identification credentials can be used, like pre-recorded "secret" information about the user as the mother maiden name (which is not so secret and so does not work so well for security), or the use of an already established different channel to send an identification code, like an SMS with a numeric key.

---

5 A previous approach was to collect some private information on the user, like names of relatives, pet animals, preferred vacations places etc., and ask this information as secondary authentication credentials to allow the user to establish a new password.

The risks of password reset

Password reset is a needed feature of current authentication mechanisms, but it is easy to abuse and provides often an simple attack surface.

The first reason for this is that there is no standard approach to password reset policies and mechanisms between companies and service providers. Many password reset services, once abused, can lead at least to a leak of information, so that by chaining information gathered through exploiting various authentication services, the attacker is able to reach his target which a first sight looked well protected.

For example, imagine a person having multiple email accounts one of which allows to reset the password providing the answer to the personal secret information, like the mother maiden name. In many cases, thanks to the social networks and the trove of information that can be found therein, the attacker can find the answer to the personal secret questions, proceed to reset the email account password and take possess of the email account.

By looking to the emails present in the account, the attacker finds evidence that the email account is used as a reset mechanism for an online service. The attacker proceeds to reset the online service password, receives the email of password reset in the hijacked email account, and it is able to take possession also of the online service account.

In this online service account, the attacker finds other information, like for example the numbers of the credit card used for the recurrent payments of the service. The attacker can use directly the credit card or use it for authenticate himself to another online service.

Proceeding in this way, slowly the attacker can gain enough information to impersonate the user and perpetrate an identity theft, or he can have access to data and information of very high value, for business, personal or even state and military reason.

Another approach to abuse password reset services is through Social Engineering. The attacker contacts the help desk of the service he wants to abuse saying that he is the user and that he has changed his email address or mobile phone telephone forgetting to update the information in his account. Moreover, now he also has lost the password but that he cannot reset it since he has not access to the old email / telephone. The attacker has to convince the help desk that he is the user,

and if he succeeds in changing the email / telephone address to his own, then he can reset the password and take over the service.

Conclusions

Passwords have been with us for a long time, and no final solution has been found yet to get rid of them. This implies that we'll have to keep using them for quite some more time to authenticate users to IT services.

But we can do something right now to minimize the risks of using passwords. The providers of IT services should work more to establish common practice on handling authentication and password management. Already many initiative have been started and some results have been obtained, but a lot to do remains.

Users can not be held responsible with understanding the risks inherent with password management, but at least should be informed and should adopt common good practices, like to identify sensitive services and manage the password to access them with particular care, isolating the access to these services from all other authentication procedures.

References

[1] CESG-CPNI, "Password guidance: simplifying your approach", https://www.gov.uk/government/publications/password-policy-simplifying-your-approach

[2] See for example: "Biometrics: Physical Attributes vs. Behavioural Patterns – The Privacy Debate", https://digitalforensicsmagazine.com/blogs/?p=1021

[3] See for example: "Hacking tool swipes encrypted credentials from password manager", http://arstechnica.com/security/2015/11/hacking-tool-swipes-encrypted-credentials-from-password-manager/ , "Dangerous Android banking bot leak signals new malware wave: GM Bot can rip creds, steal SMS and phone two factor tokens" http://www.theregister.co.uk/2016/02/23/dangerous_android_banking_bot_leak_signals_new_malware_wave/

[4] One of the first examples of such malware was "ZeuS Mitmo (man-in-the-mobile) ", see for example "ZeuS attacks mobiles in bank SMS bypass scam",

http://www.theregister.co.uk/2010/09/27/zeus_mobile_malware/

[5] See for example: “Brian Krebs criticises PayPal’s security as authentication flaws exposed” http://www.theregister.co.uk/2015/12/30/krebs_paypal_hack_criticism/ ,
“Face facts about Internet security”, Bruce Schneier
http://edition.cnn.com/2015/10/23/opinions/schneier-cia-hacking-security/index.html

Andrea Pasquinucci (PhD CISA CISSP)