"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XIX – 2016 – Issue 1
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in: PROQUEST / DOAJ / DRJI / JOURNAL INDEX / I2OR / SCIENCE LIBRARY INDEX / Google Scholar / Crossref / Academic Keys / ROAD Open Access / OAJI / Academic Resources / Scientific Indexing Services / SCIPIO

AUTHENTICATION - THREATS AND COUNTERMEASURES

Eduard Eusebiu EMANDII[1]
[1]Mircea cel Batran Naval Academy, no. 1, Fulgerului Street, Constanta, Romania

***Abstract**: When it comes to cybersecurity, one of the most sensitive issues is the user's credentials. Obtaining a user's password is the easiest way for a hacker to gain control of a system or stealing personal information. Nowadays more and more services tend to be online from stores, courses, bank transactions to ways of socializing. For all of this we need a user account and password to authenticate.*
Using a different password for each account can become tedious so we tend to use simple and short passwords in order to retain them, but with increasing number of accounts we arrive at the same result by using the same password namely for all online resources to which we have access. This is the first step of becoming an easy target to get hacked.This paper aims to outline some methods of increasing security when it comes to authentication

***Keywords**: authentication, security, cyber defence, cybersecurity*

Authentication is the process to determine if someone is who pretend to be. So, in order to establish if someone can access some information he must undergo an authentication process.
Considering the factors of authentication, the ways in which someone can be authenticated is divided into three main categories: something the user *knows*, something the user *has*, and something the user *is.*

- the knowledge factors (something the user knows): password, pass phrase, personal authentication number (PIN), shared secret;
- the ownership factors (something the user has): security token, ID card, software token;
- the inherence factors (something the user is or does): fingerprint, retinal pattern, signature, face, voice, unique bio-electrical signals.

Taking into account the three factors we can have multiple types of authentication:

- single factor authentication: using one method of authentication;
- two factor authentication: using two different types of authentication mechanism to authenticate;
- multiple: using multiple forms of the same factor. (Password + identifying an image).

The knowledge factors
Password Authentication
Password authentication is the common method to prove your identity and it is used on most web application. Although is not the safest method, it is the easiest way to authenticate. It is widely used on computers, bank accounts, web accounts and more.
Generally, passwords are not stored in plain text, they are stored as hashes. A hashed password is an encrypted password which can't be decrypted and is known as *one-way-encryption* method. These systems very often use MD5 or SHA1 to hash the passwords. So, in Windows operating system, password are stored in the SAM file, while in Linux are stored in the /etc/shadow file and for web application/services the passwords are stored in a database like MySQL, Postgre SQL, Oracle etc. In all cases you can use a service or a file that has root privileges to grab those passwords.
Types of attacks
Dictionary
The "dictionary attack" is the most simple attack mode, also known as "Wordlist attack". This method is based on trying some strings in a pre-arranged list, in most cases derived from a list of words such as a dictionary. Dictionary attack often succeed because most users tend to use simple passwords that are ordinary words, or simple variants obtained, for example, by appending a digit or punctuation character.
There are a lot of software and dictionary which can be found on Internet and which can be used by everyone in order to crack your account in a mere of minutes.
Defeating dictionary attack is relatively easy by not using a simple word ora combination of words which can be found in a dictionary.
Rainbow table
Almost all systems store the password in a hash. This means that even if you can get the files with the account passwords, you get them encrypted. A method to crack this encryption is by taking dictionary files used on the first method and hash each word and compare it to the hashed password. The disadvantage of this approach is that it requires more time and resources to CPU.

DOI: 10.21279/1454-864X-16-I1-063

To speed up the process of decryption you can take a table with all words in the dictionary already hashed and compare the hash from the password file to your list of hashes. If there is a match you will find out the password.

Brute force

This method is the most time consuming for password cracking. Brute force is an exhaustive key search by attempting all possibilities of all letters, numbers, special characters that can be combined.

Nowadays it is quite difficult as a brute force attack to succeed on a web service, considering the security measures that could be implemented, such as requiring a CAPTCHA code to confirm the existence of a person who tries authentication and up to IP blocking after a limited number of failed login attempts. So, this type of attack is more efficient if it is done offline by grabbing the encrypted password file and trying to decrypt on a local computer.

Hybrid

Hybrid password attack uses a combination of dictionary words with special characters, numbers, etc. Often these hybrid attacks use a combination of dictionary words with numbers appending and prepending them, and replacing letters with numbers and special characters. Forinstance, a dictionary attack would look for word *"password"*, but a hybrid attack might look for *"p@$$w0rd123"*.[1]

Passphrase

A passphrase is a string which is usually longer than a password that is used in creating a digital signature (an encoded signature that proves to someone that it was really you who sent a message or who authenticates).[2]

Passphrases are often used to control both access to, and operation of, cryptographic programs and systems. Passphrases are particularly applicable to systems that use the passphrase as an encryption key.[3]

The main difference between passphrase and password is that when it comes to passphrases you can use multi string phrase including spaces and tabs. Normally, password is a single string andmany application will braks with spaces and tabes while using authentication.[4]

For example, a password could be like this: *aYtG%$fY!hsdhf&qQ*and a passphrase would look like this: *Yb@ ytgd!23 56er$$T odg!Tr*.

The main advantage in using passphrases is that you can use spaces and tabs which is a good countermeasures for breaking password authentication. This is making dictionary based attack quite difficult.

PIN

A Personal Identification Number is a numeric password used to authenticate in a system. It is usually used on accessing automated teller machines (ATMs). The string it is between 4 -12 characters long. Not being very complex, the systems which uses this type of authenticationhas implemented as a countermeasure, the capability to block the user account after three failed attempts to login.

Shared Secret

A shared secret is used as a cryptography mechanism which provide secure communication between two or more parties. Without a shared secret among the parties, there is no way for each party to guarantee the identity of the other.

As an example of using shared secret is when serves as a password between:

- A RADIUS client and a RADIUS server;
- A RADIUS client and a RADIUS proxy;
- A RADIUS proxy and a RADIUS server.

So, in order to mitigate eavesdropping when sending username and password in plain text it is a good practice to use shared secret.

A disadvantage in using shared secrets is on the process of distribution because there is the risk of forgery and tampering.

The ownership factors

Security Token (authentication token)

Security token is a small hardware device that the owner carries to authorize access to a service or a network. The security token can replace the password used by the user or can be used in addition to the user account and password which is called *"2 Factor Authentication"*.

Even if the token is lost by the owner, it can't be used without the PIN.

There are three main security token types[5]:

- Connected token: this type of token requires a physical connection to generate automated authentication data transfer. It is also requires special installed host input devices. Most used hardware support for this type of tokens are USBs and smart cards;
- Disconnected tokens: this token is most common for two-factor authentication and usually requires a PIN before generating authentication data. It is not physically or logically connected to a host computer but displays a randomly generated code on a built-in display, which is usually called *One-time-password (OTP)*;
- Contactless tokens: this is rarely used because is not physically connected to the host computer but uses a logical connection instead for authentication data transmission. For example, radio-frequency identification (RFID) tokens are

DOI: 10.21279/1454-864X-16-I1-063

based on contactless tokens but are still under development. So, due to security concerns, RFID usage is limited.

Electronic identification card

eID is a physical identity card that can be used for online and offline authentication, giving access for benefits or services provided by government authorities, banks or other companies.

Countries which currently issue government-issued eIDs include Belgium, Bulgaria, Germany, Israel, Italy, Luxembourg, the Netherlands, Mexico, Morocco, Pakistan, Portugal, Romania, Estonia, Latvia, Lithuania, Spain, Slovakia, Malta, and Mauritius. Sweden and Finland accept bank-issued eIDs (also known as BankId) for identification by government authorities.[6]

In order to authenticate with an eID, an online service provider triggers the client software through a browser plugin and hands over to the eID server to authenticate the owner of the eID:

After this process, control returns to the service, which uses the authentication result for its purpose.

Software token

Software token is usually used in a two-factor authentication process and is stored on an electronic-device such as a desktop computer, laptop, PDA or mobile phone.

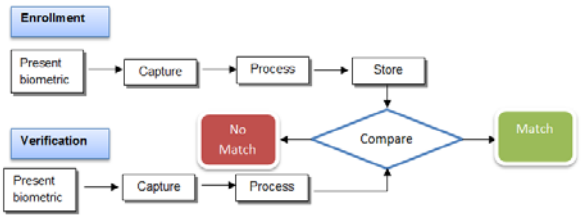
Because it is only as a logical form and not a physical one, it is exposed to the risk of duplicating through a computer viruses and software attacks.

Software token can be seen as an attempt to replicate the security advantages of security token, while simplifying distribution and lowering costs. A smartphone soft token app performs the same task as a hardware-based security token, but taking into account that smartphones are connected devices it makes them inherently less secure. So, the security environment depends on the device's operating system and client software.

Theinherence factors

The inherence factors uses biometrics to automated recognition of individuals based on their biological and behavioral characteristics.

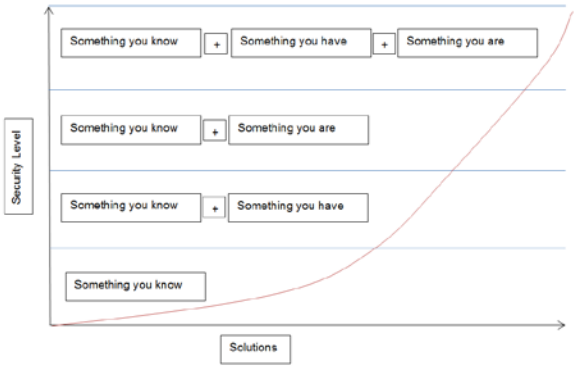
How do biometrics work?



The advantages of using biometrics are that they cannot be forgotten, lost, shared or stolen. They also replace vulnerable passwords, are convenient because there are nothing to carry or remember and is also cost saving by reducing helpdesk support for password resets.

CONCLUSIONS

As you can see there are a lot of methods ofauthentication but everyone has his weaknesses and strengths. The figure bellowshows that the most secure method is multifactor authentication because combines all types of authentication [7].



Using only password to authenticate is not so secure because users tend to use simple password to be remembered and which can be easily cracked. On the other hand the usercan be constrained to setup a complex password by using long string containing alpha-numeric and signs but in this situation there is the temptation to note the password on a piece of paper and thus be exposed to unauthorized persons.

The most used techniques for stealing the identity of a user and getting access to their most sensitive systems and data is by password guessing and impersonation.

Impersonation is a social engineering technique used for instance by an attacker who calls the helpdesk pretending to be an employee, claiming he forgotten his password and ask the helpdesk to reset it.

DOI: 10.21279/1454-864X-16-I1-063

That is way most of the online services tend to use two-factor authentication or one-time-password (OTP) instead of single one authentication, ensuring a better security.
As a checklist for securing authentication there are some recommendation to follow [8]:

- Using passphrases rather than passwords;
- Deploy two-factor authentication for privileged users and for remote access;
- Permit password resets only with call-back and PIN or cherished information authentication;
- Helpdesk staff should be encouraged to withhold support when a calldoes not feel right;
- Train all users as an ongoing process;
- Test the company's ability to protectits environment

Authentication is the first target of an attacker who tries to gain access to an application or service and that's wayis considered the central security mechanism to defend itself.

BIBLIOGRAPHY

[1] http://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-1-principles-technologies-0156136/
[2] http://searchsecurity.techtarget.com/definition/passphrase
[3] https://en.wikipedia.org/wiki/Passphrase
[4] http://www.cyberciti.biz/tips/openssh-difference-between-password-passphrase.html
[5] https://www.techopedia.com/definition/16148/security-token
[6] https://en.wikipedia.org/wiki/Electronic_identification
[7] http://www.biometrics.org/bc2014/presentations/Mon_1516_Tilton_1400.pdf
[8] http://www.computerweekly.com/feature/How-to-ensure-strong-passwords-and-better-authentication

DOI: 10.21279/1454-864X-16-I1-063