IMPROVING QUALITY OF AUTHENTICATION

POBOLJŠANJE KVALITETA AUTENTIKACIJE

M.Sc. Suad Sućeska
Sarajevo
Bosnia and Herzegovina

REZIME

This article works with influence of new types of authentication to quality and data access security. By expanding the use of information technology to various activities and public services, the process of authentication becomes more and more important. However, number of those who want to abuse the benefits of ICT technology is also greater, and their professional level to achieve that is higher. That is why is working so much on the safety of using ICT technology. This also applies to authentication, as an access procedure, which is as such very much exposed to abuses.

Keywords: authentication, quality, data security.

ABSTRACT

Ovaj članak obrađuje uticaj novih vrsta autentikacije na kvalitet i sigurnost pristupa podacima. Sa širenjem upotrebe informacione tehnologije na razne djelatnosti i javne servise proces autentikacije postaje još važniji. Međutim, veći je broj onih koji žele zloupotrebiti pogodnosti IKT tehnologija, a sve viši je njihov stručni nivo kojim to žele postići. Zato se mnogo radi i na sigurnosti upotrebe IKT tehnologija. Ovo se odnosi i na autentikaciju, kao pristupnu proceduru, koja je kao pristupna jako mnogo izložena zloupotrebama.

Ključne riječi: autentikacija, kvalitet, sigurnost podataka

1. INTRODUCTION

Process of authentication is necessary to differentiate one particular from many registered users for access to some electronic content, that is the operating system or application determines whether right user attempted to access. For MS Windows operating systems authentication is doing using the SAM (Security Account Manager) database for local and remote users. This authentication process is additionally protected with NTLM (NT LAN Manager) protocol. Starting with MS Windows 2000 SP4 remote users are authenticated using Active Directory (AD).[3,8] The authentication data used for a particular user account for this type of authentication is a password. Applications, local and Web, are also designed to require authentication before getting an access. Data for these types of authentication are used from the SAM database, AD, or database of user accounts made for a particular application. From the very beginning of the user authentication, various ways of obtaining another user's account data (name, password) have been found to access to LAN or an application as that user. Abuse is often a reason for these activities.

2. NEW TYPES OF AUTHENTICATION

Using computers in various businesses has led to new, more secure types of authentication. This is particularly evident when using computers and the Internet in banks. For a long time banks have been competing in offering various Internet and, more recently, mobile services to their clients. Using passwords for these services is not safe enough. Therefore, the following types of authentication are made: token authentication (a token with a USB stick, a special token generator), a bank card, a key.

Figure 1. Token generator

In recent times, efforts are being made to reduce the probability of guessing authentication data. Authentications using personal characteristics are made for this purpose. On this way are made authentications which use: fingerprint, iris, voice, typing speed, keystroke interval, Face ID. For some of the aforementioned authentications is also calculated the probability of guessing. The probability of guessing for fingerprint authentication (Touch ID) is
p = 1: 50.000, and for Face ID probability of guessing is p = 1: 1.000.000.000.[14] These data also contribute to the simplicity and speed of authentication, because instead of the password, with minimum length of 8 characters to be typed, it uses personal characteristics which can be immediately obtained using a camera or microphone.

3. ADVANTAGES OF NEW TYPES OF AUTHENTICATION

Identity theft precedes to the theft of data and money through the Internet. Therefore, security of the authentication process is enhanced with Two-factor Authentication (2FA). This method requires two unrelated information instead of entering a personal identification information (password). It uses personal information: something what is known (password); something what you have (bank card, cell phone); personal characteristics (fingerprint, voice, iris).[11] This method is safe even if someone, who wants to use it, knows one of two authentication data.

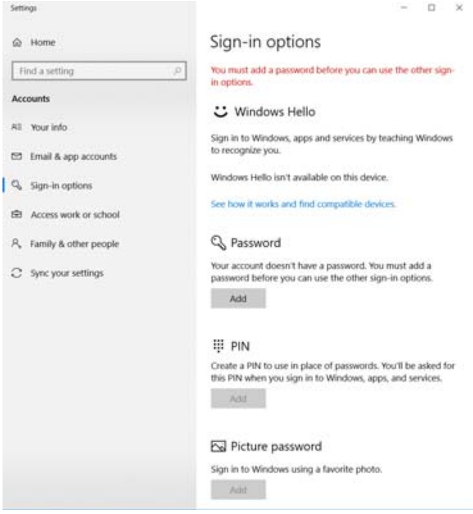
Examples of 2FA are:

- Bank card and pin. It is necessary to have a bank card and to know appropriate pin.
- The password and the sending of a one-time code in the message to the mobile phone number entered as a personal data. It is neccessary to know password and to enter an one-time code sent in the message to your mobile phone.
- The password and confirmation of request sent in e-mail message to the e-mail address that had been given as personal data.

The 2FA method is slower than the authentication method which uses only the password, and it also requires a mobile phone with the appropriate number for getting an one-time code which has to be entered during authentication.

2FA authentication is currently good protection for important personal information on the Internet. Web services: Google, Facebook, Amazon, Microsoft, Twitter use 2FA authentication.[10]

Microsoft Windows 10 includes a multi-factor authentication system named Windows Hello. This authentication, besides privacy protection by password, provides authentication capabilities using: fingerprint, eye iris, face image, and others.



Sign-in options

You must add a password before you can use the other sign-in options.

Windows Hello

Sign in to Windows, apps and services by teaching Windows to recognize you.

Windows Hello isn't available on this device.

See how it works and find compatible devices.

Password

Your account doesn't have a password. You must add a password before you can use the other sign-in options.

PIN

Create a PIN to use in place of passwords. You'll be asked for this PIN when you sign in to Windows, apps, and services.

Picture password

Sign in to Windows using a favorite photo.

Figure 2. Options for authentication configuration in MS Windows 10

To use authentication with Windows Hello, it is neccessary to provide the appropriate hardware: a fingerprint reader, an iris and face recognition camera. Windows Hello can be configured from the box 'Sign-in options', on Figure 2, which is obtained by click on the Start, Settings, Accounts.

The authentication using personal features with Windows Hello is 3 times faster than password authentication.[11] The applications that can currently use Windows Hello authentication are: Dropbox Explorer; Enpass; 8 Zip; Cloud Drive !; OneDrive; FourBudget; ShareFile; One Messenger; OneLocker Password Manager; Flow Mail; Hopic Explorer.[5] This type of authentication besides speed also gives a higher degree of security. Biometric technologies use personal characteristics, and their probability of guessing are:

- probability of guessing for the authentication using finger print: p= 1:50.000,
- probability of guessing for the authentication using Face ID: p= 1:1.000.000.000.[14]

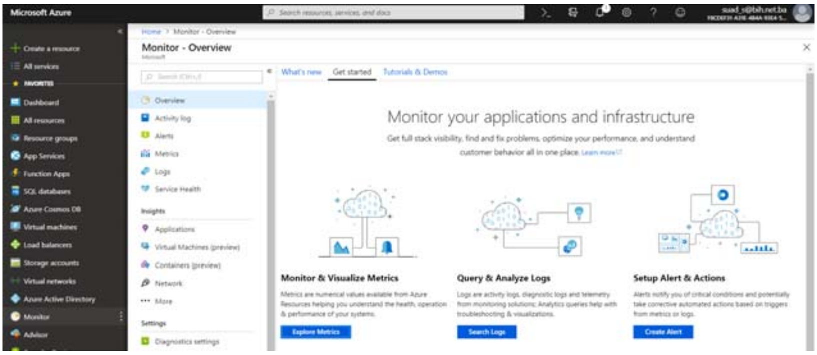
Since 2017. Apple has been using biometric authentication technology by fingerprint: Touch ID. In 2018., this company introduced new technology: TrueDepth, which is built into the front camera. This biometric technology is used for authentication during unlocking the smartphone. The picture made by front camera using TrueDepth is compared with the 3D map of the face stored in the smartphone. This biometric authentication technology is called the Face ID. The Face ID determines whether a smartphone will be unlocked or not by comparing of the image made by the front camera with appropriate 3D map stored in the smartphone's processor.[9]

Authentication can also be done using QR code (two-dimensional bar code). So, to use WhatsApp on computer (WhatsApp Web) it is neccessary to open WhatsApp on your smartphone, after that to chose the WhatsApp Web from the Menu or the Settings, and then to authenticate using smartphone and QR code from the Web site.

3.1. Single sign-on

The Single sign-on (SSO) is an authentication benefit, which greatly simplifies access to a large number of applications and resources. Instead of signing in with a user account and password for access to every single application or resource, it is neccessary to sign in just once to access to all applications and resources. SSO is the Microsoft's authentication benefit for access to aplications and resources, which is embedded in MS Azure Active Directory.[15]

This is an important benefit for companies using SaaS (Software as a Service) on the Azure cloud platform. This is also important for companies that link a Active Directory in private domain with Active Directory in public Cloud where they have some applications and resources. SSO enables to log on Active Directory (AD) in the local domain, but to have access to the applications and resources of that company on the local domain and on Azure public Cloud with Azure AD too.



Monitor your applications and infrastructure

Get full stack visibility, find and fix problems, optimize your performance, and understand customer behavior all in one place. Learn more

Metrics are numerical values available from Azure Resources helping you understand the health, operation & performance of your systems.

Logs are activity logs, diagnostic logs and telemetry from monitoring solutions; Analytics queries help with troubleshooting & visualizations.

Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

Figure 3. The Microsoft Azure Portal

SSO is working for applications that support any of the following authentication protocols: SAML 2.0, WS-Federation, or OpenID connect. This includes the following applications: Box, Citrix, Concur, Docusign, Dropbox for Business, Dynamics CRM, Google Apps, Jive, Office 365 Exchange Online, Office 365 SharePoint Online, Salesforce, ServiceNow.[7]

4. CONCLUSION

Authentication needs to be better in order to better protect privacy of a user when accessing a to computer or Internet resource. The first type of authentication using user account and password has become insecure. Therefore authentication security is enhanced with new types of authentication: 2FA (Two-factor Authentication), fingerprint, iris, voice, typing speed, keystroke interval, Face ID, Windows Hello. Paralel with improving security, there are also works on simplifying of the authentication process for the access to computer and Internet resources. Some of these improvements include: Single sign-on, QR code authentication, face, fingerprint, voice.

5. REFERENCES

[1] Authy, https://www.bug.hr/appdana/authy/996.aspx, Bug, 23.7.2014.

[2] FIDO Alliance: FIDO Alliance, https://en.wikipedia.org/wiki/FIDO_Alliance

[3] Microsoft: Microsoft NTLM, https://docs.microsoft.com/en-us/windows/desktop/secauthn/microsoft-ntlm

[4] Microsoft: What is Windows Hello?, https://support.microsoft.com/en-us/help/17215/windows-10-what-is-hello

[5] Microsoft: Windows Hello: Discover facial recognition on Windows 10, https://www.microsoft.com/en-us/windows/windows-hello

[6] https://en.wikipedia.org/wiki/Windows_10

[7] Microsoft: Enterprise Single Sign-On, https://docs.microsoft.com/en-us/host-integration-server/esso/enterprise-single-sign-on1

[8] Single sign-on, https://en.wikipedia.org/wiki/Single_sign-on

[9] Dragan Petrić: Apple iPhone X - Nedovršena revolucija, https://www.bug.hr/recenzije/apple -iphone-x-nedovrsena-revolucija-1503, Bug, 1.11.2017.

[10] Zašto biste trebali koristiti dvostruku autentifikaciju?, https://pcchip.hr/helpdesk/zasto-biste-trebali-koristiti-dvostruku-autentifikaciju/, PCChip, 28.04.2017.

[11] Blaž Jurišić: Security - moderni načini autentikacije, https://www.bug.hr/microsoft/security-moderni-nacini-autentikacije-3859, Bug, 19.04.2018.

[12] Autentikacija, https://hr.wikipedia.org/wiki/Autentikacija

[13] QR Code, https://en.wikipedia.org/wiki/QR_code

[14] Face ID, https://en.wikipedia.org/wiki/Face_ID

[15] Microsoft: Single sign-on, https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on