ANALYSIS OF APPLICATION OF AUTHENTICATION METHODS IN THE PROTECTION OF USER ACCOUNTS

Tamara Milić[1] Biljana Radulović[2] Valentina Bozoki[3] Nemanja Tasić[4] Igor Vecštejn[5]

Abstract: In the age of modern civilization, when visiting people on the Internet is classified as a daily routine, the security of user accounts has never been more important. The Internet, as a source of large amounts of data, poses a risk of various cyber threats. The security of user accounts has become an indispensable segment of cyber security because unauthorized access can lead to serious consequences for the user. Inadequate protection of user accounts provides an opportunity for attackers to compromise accounts and access confidential information with minimal effort. One form of cyber threats phishing attacks, which are considered one of the most common methods of data theft. Phishing attacks are one of the forms of cyber attacks, where users are sent fake e-mails that appear to be sent from a relevant source, with the aim of "stealing" vulnerable data from users, such as credit card numbers, passwords, etc.

Key words: Simple Authentication, Two-factor Authentication, Analysis, Accounts, GoPhish, Users

1. INTRODUCTION

Authentication is the process of determining whether an entity should be allowed access to the system (an entity can be a person, process or application, computer, device, etc.). If the entity is allowed access to the system, authorization follows - a process in which the rules for accessing system resources are determined [1]. Figure 1 shows how authentication and authorization differ.

Figure 1 – An Example of Authentication and Authorization [2],[3]

Based on Figure 1, authentication identifies who the user is, and authorization represents a kind of permission to the user who has identified himself. Users who use online shopping, when they create their user account in the online store, have access to account settings, payment details, account history, etc. On the other hand, online store administrators have some other permissions in addition to the options mentioned above, such as review of goods, entry of new services, products, change of price list, and similar [2].

A computer system can authenticate a user based on an authentication factor [4]:

- Something he knows (knowledge factor) - most often it is a username and password, but it can also be, for example, "the date the student graduated", etc.

[1]University of Novi Sad, Technical Faculty "Mihajlo Pupin"; Djure Djakovica bb, Zrenjanin, tamara.milic@tfzr.rs
[2]University of Novi Sad, Technical Faculty "Mihajlo Pupin"; Djure Djakovica bb, Zrenjanin ,biljana.radulovic@tfzr.rs
[3]University of Novi Sad, Technical Faculty "Mihajlo Pupin"; Djure Djakovica bb, Zrenjanin , valentina.bozoki@tfzr.rs
[4]University of Novi Sad, Technical Faculty "Mihajlo Pupin"; Djure Djakovica bb, Zrenjanin, nemanja.tasic@tfzr.rs
[5]University of Novi Sad, Technical Faculty "Mihajlo Pupin"; Djure Djakovica bb, Zrenjanin, igor.vecstejn@uns.ac.rs

- Something that has (possession factor) – an obvious example is a key or payment card, token, USB dongle, and the like
- Something that is (factor of inherence) - this includes biometric data, such as fingerprint, facial appearance, retina of the eye (scanned), voice color. It also includes behavioral biometric data such as the way you walk, typing on the keyboard, the way you pronounce words, etc.
- Where I am (location factor) - most often determined using the GPS on the mobile phone, the IP address from which it is accessed (if authentication is done via the Internet) or even by determining the fact that a person has entered a monitored restricted area (for example using fixed telephone lines from the office, police station, presidential office...)
- At what time is authentication performed (time factor) - it represents limiting access to the system outside of a certain time interval, assigning keys/tokens with short, limited time duration, etc.

2. CLASSIFICATION OF AUTHENTICATION METHODS

Authentication methods are divided according to the method of verifying the user's identity on [5]:

- Traditional methods or knowledge-based authentication - Simple authentication
- Authentication by possessing physical objects or devices - Two-factor authentication
- Biometric authentication methods that use physiological or behavioral characteristics – Multi factor authentication

Figure 2 shows the mentioned types of authentication, as well as the factors on which each of them is based.

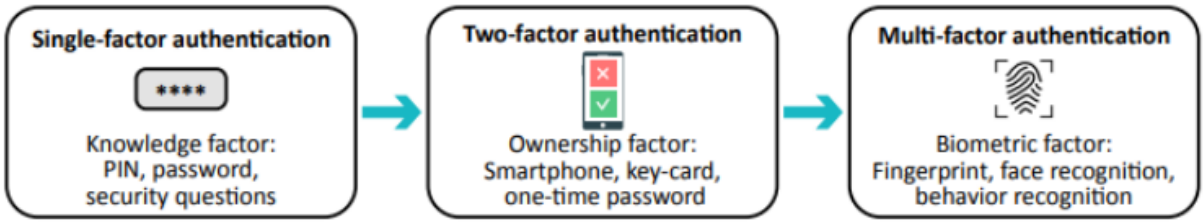

Figure 2 Evolution of authentication methods from simple to multi-factor [2]

1.1. Simple Authentication

Simple authentication (Basic authentication or Single-factor authentication, SFA) is based on a single password. A password can be any information used to verify a person's identity. The most common examples that fall into such a category are: shared passwords, host and system names, application names, numeric ID, etc. The authentication process is often performed as a plaintext comparison where the given password exactly matches the expected password or with some permutation function where the password is first subjected to a modification such as encryption and the resulting data is then compared [2],[6]. Simple authentication is not very secure and can be easily stolen because hacking technology has become more diverse and advanced, and security and authentication cannot rely only on ID and password based authentication [7]. Figure 3 shows an example of simple user authentication.

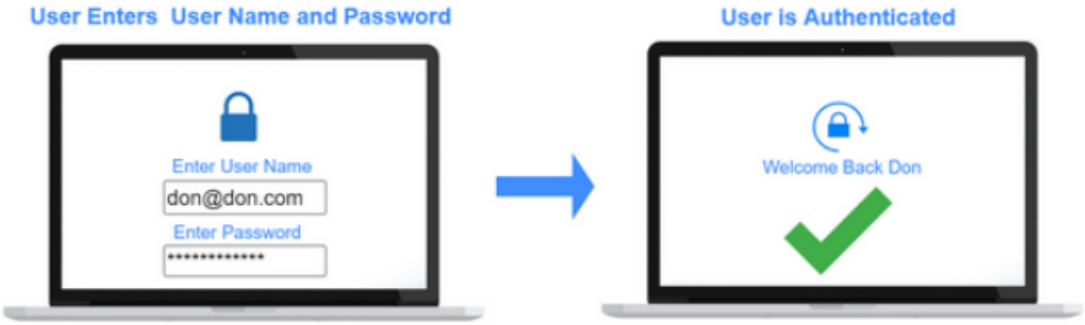

Figure 3 - Example of simple user authentication [2],[6]

1.2. Two-factor authentication

Two-factor authentication (2FA) is a bit more complex than simple authentication because it uses two combinations to verify the user's identity. It requires the user (whose identity needs to be verified) to provide something they know, such as a PIN or password, and something else they have, such as a bank card. That is why the most common example of two-factor authentication is an ATM that requires a bank card and a personal identification number (PIN) that serves as a password [2]. The advantage of two-factor authentication over simple authentication is that if an attacker "steals" the password, he still can't access the account because he needs another identification that he can't get. Figure 4 shows two-factor user authentication.

Figure 4 - Example of two-factor user authentication [2],[6]

A 2015 survey showed how many companies have started using two-factor authentication on the Internet. Based on the results, it can be assumed that the number of companies using two-factor authentication is increasing, because it can be seen that in 2011, only three service providers used two-factor authentication, and already in 2014, the number of service providers using two-factor authentication jumped to even 19 [2]. Figure 5 shows the time period of the beginning of the use of two-factor authentication on web pages and web services.

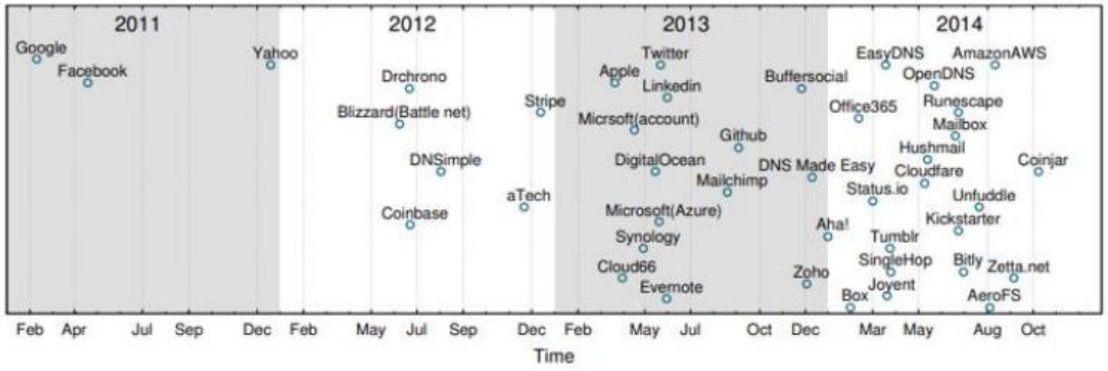

Figure 5 - Time period of using two-factor authentication on web pages and web services [2],[9]

•

1.3. Multi-factor Authentication

Multi-factor authentication implies a method of protecting the user's account, where the user needs to use another type of account protection (verification code, SMS message,...) in addition to the password. In other words, for authentication to be considered multi-factor, the user must possess a minimum of two different authentication factors. Figure 6 shows multi-factor authentication.

Figure 6 - Example of multi-factor user authentication

On the other hand, the biometric authentication method requires the user to confirm his identity with his physiological or behavioral characteristics, that is, it is based on the factor of inherence or belonging, i.e. "something that is". Physiological characteristics are: fingerprint and face recognition; while behavioral recognition: voice, gait, keystroke scanning, and signature scanning [5].

2. METHODOLOGY

The aim of the research of this paper is to highlight the importance of authentication in protecting user accounts from phishing attacks. Two authentication methods are used:

- Simple authentication - log in using a username and password
- Two-factor authentication (2FA) - login using a username, password, and an additional security code (sent via SMS)

The GoPhish software was used for the simulation, which is used to simulate phishing attacks. GoPhish enabled detailed management of the entire course of this research, which included: processes of creating and sending phishing emails, monitoring user interaction with sent emails and generating a detailed report on user behavior, monitoring opened emails, and clicks on phishing links. The research consisted of two phases:

- First stage: defining the target groups of users based on the type of authentication. 2 groups of five users each were formed. Users in the first group used simple authentication, and users in the second group used two-factor authentication. In the GoPhish software, an email with the title "Business Offer" was created, which contained a link to a phishing page. Mail contained a page layout, where the user had to enter their user account login details and then their personal details. One email was sent to each user. After sending the emails, certain metrics were monitored, such as the number of opened emails, clicks on the phishing link, and the number of entered data on the page marked as phishing.
- Second phase: data collection. The total number of e-mails sent is 20 (one e-mail per user). Diagrams are generated in Excel.

The metrics that were used in the analysis are:

- Opened emails – Number of users that have opened phishing mail
- Click on link – Number of users that have clicked on a phishing link that is in the content of mail
- Entered data on phishing page – Number of users that have entered their data (username and password) on simulating page
- Identification of compromised accounts – User has entered a username and password on the phishing page (simple authentication) and for 2FA additional security code was sent as an SMS on mobile of the user.

A user account is considered compromised if all required data that is in the form (username, password, and possible 2FA code) are entered correctly. In the case of 2FA, if a user entered only a username and password without providing additional code, in this particular case SMS, then the account is not considered compromised.

3. DISCUSSION

Figure 7 shows the total number of opened and unopened emails sent to users via the GoPhish tool for the first group, expressed in percentages.

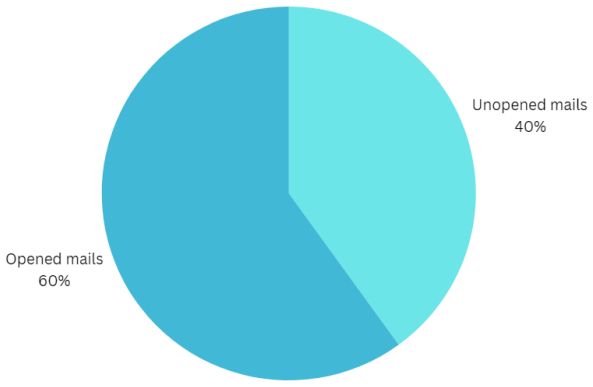

Figure 7 - Display of the relationship between open and unopened mail for the first group expressed as a percentage (%)

Figure 8 shows the total number of compromised accounts for the first group, expressed as a percentage. Accounts of users who entered confidential information necessary to log into their user accounts were compromised.

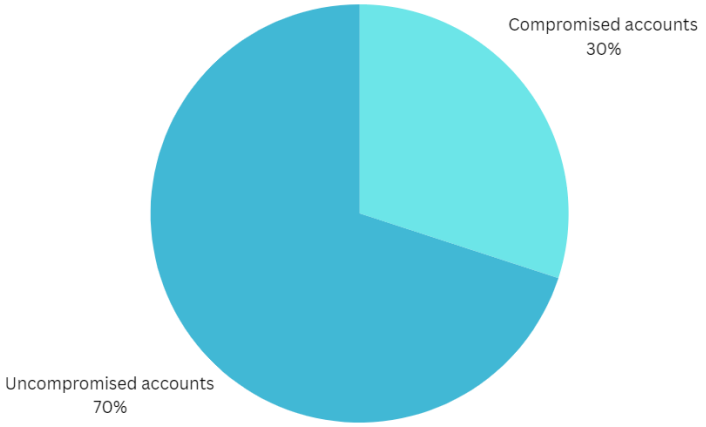

Figure 8 - Display of the relationship between the number of compromised and non-compromised user accounts of the first group, expressed as a percentage (%)

Figure 9 shows the total number of opened and unopened emails sent to users via the GoPhish tool for the second group, expressed in percentages.

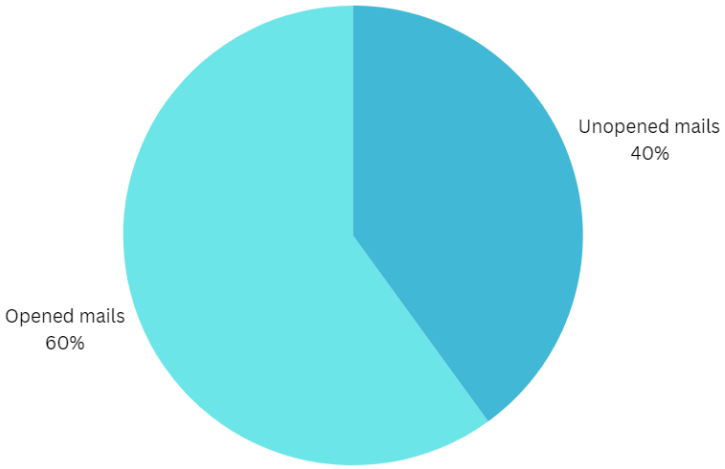

Figure 9 - Display of the relationship between open and unopened mail for the second group expressed as a percentage (%)

Figure 10 shows the number of users from the second group who, after clicking on the phishing link, entered their password in the form, expressed as a percentage.

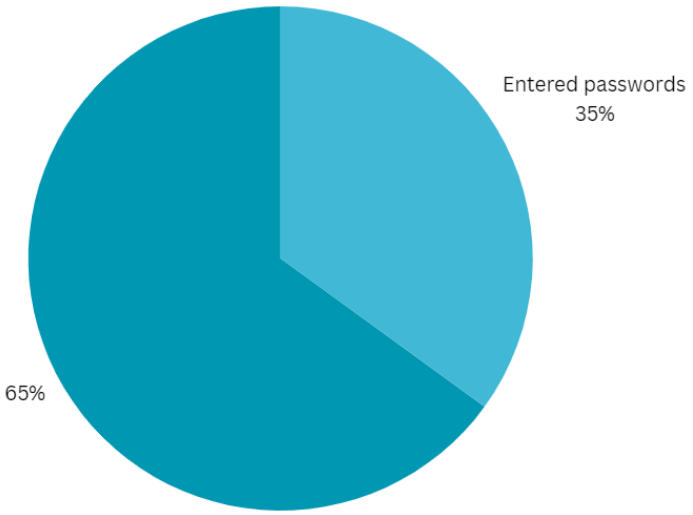

Figure 10 - Display of the relationship between the number of entered and unentered passwords in the form for the second group expressed as a percentage (%)

It is concluded that by applying the two-factor authentication method, the accounts were not compromised, because they were additionally protected with another authentication factor (verification code, sent via SMS). Therefore, the number of compromised accounts is zero.

4. CONCLUSION

The research results show that with the help of two-factor authentication, the number of compromised accounts is reduced compared to simple authentication via username and password. The first group, which used the simple authentication method, had three compromised accounts, while the second group, which used two-factor authentication, did not have a single compromised account. This can confirm the high degree of efficiency of two-factor authentication as an additional security measure that makes it difficult to compromise data, even when users tend to open phishing emails and click on links found in the contents of the mail.Although two-factor authentication can provide a high level of protection for user accounts, the risk of compromising accounts protected by this authentication method still exists. One of the vulnerabilities is precisely caused by phishing attacks because users can in some cases be deceived by attackers and thus reveal their one-time codes through fake mail. Therefore, as a precautionary measure, it is necessary to include simulations of phishing attacks so that users know how to recognize an email that was sent by a relevant source versus one that was not.The simple authentication method does not provide a sufficient level of security, because users are subject to an increased risk of phishing attacks due to insufficient education about phishing attacks. Therefore, it is necessary to improve the security of user accounts with another authentication factor. On the other hand, it is necessary to use any authentication method for the security of user accounts, because even simple authentication that requires entering a username and password is the first line of defense against unauthorized access. With a user account without any authentication, an attacker can easily access data and thus expose the user himself or the company to a great risk of financial losses, leakage of confidential information, loss of reputation, etc.

Considering these findings, the implementation of robust authentication methods is particularly critical in the fashion and textile industry, which is increasingly dependent on e-commerce platforms and vulnerable to cyber threats. These industries are now more and more moving to virtual transactions and hence have become easily influenced by online scams. Going forward, the security and authentication of user accounts in this sector should be directed at safeguarding client data through the advancement of safety procedures, such as biometric and behavioral authentication, which will provide protection against unauthorized access. This is particularly relevant given the industry's increasing reliance on e-commerce platforms, where sensitive customer data, including payment information, is frequently handled. Implementing adaptive, context-aware authentication systems that

adapt security measures in keeping with user behavior, location, and device, will play a critical role in reducing fraud. In addition, the inclusion of blockchain for decentralized identity management and providing the necessary education to users on phishing threats are the ways to further toughen up security. These dynamic breakthroughs will make the sector a safe environment for end-users and businesses, thus helping in the fast digitizing process.

Also, the topic of this scientific work can serve as a reference point for some future research in the domain of authentication and adaptive systems. One of the important directions of research can be optimization of the performance of blockchain networks, where new algorithms would be used to reduce resource consumption and improve the speed of transactions, for example: Proof of Stake (PoS). The development of advanced authentication mechanisms (for example: biometric authentication and multi-factor authentication - MFA), can be a central part of the Zero Trust model research. Another direction of future research can be the development of anadaptive system that will require biometrics from the user as an additional authentication factor when he notices suspicious behavior on the user account (for example unusual location, device, etc.) or if the user simply tries to log in from a new device.

5. REFERENCES

[1] Radlovacki, V.: *„Autentifikacija“*, blog, https://www.radlovacki.com/authentication/
[2] Sabolek, I.: *„Višefaktorska autentifikacija putem dijeljenja tajni“*, Master's thesis, University of Pula, Faculty of Informatics, Pula, 2021.
[3] Bhargav, A.: *„Authentication vs Authorization – What's the difference?“*, ssl2buy, https://www.ssl2buy.com/wiki/authentication-vs-authorization-whats-the-difference
[4] Novović, R.: *„Dvofaktorska autentifikacija (2FA)“*, BikeGremlin , 2024, https://io.bikegremlin.com/12434/2fa-objasnjenje/
[5] Zrno, I.: *„Usporedba metoda autentifikacije u Web aplikacijama“*, Undergraduate thesis, University of Split, Faculty of Science, Split, 2024.
[6] DoubleOctopus: *„Single-Factor Authentication“*, https://doubleoctopus.com/security-wiki/authentication/single-factor-authentication/
[7] Kim, J.-J.; Hong, S.-P.: *„A Method of Risk Assessment for Multi-Factor Authentication“*, Journal of Information Processing Systems, 7(1), pp. 187–198, 2011, doi: 10.3745/JIPS.2011.7.1.187
[8] Okwii, D.: *„Correctly Configure Two-Factor Authentication before you're locked out of your own account“*, Dignited, https://www.dignited.com/30668/configure-two-factor-authentication-before-you-get-locked-out-of-your-own-account/ , 2018.
[9] Petsas, T.; Tsirantonakis, G.; Athanasopoulos, E.; Ioannidis, S.: „Two-factor authentication: is the world ready?“, in *Proceedings of the Eighth European Workshop*, April 2015, doi: 10.1145/2751323.2751327
[10] Syed, S.: *„Your bank account may be blocked if you don't verify biometrics before June 30“*, TechJuice, https://www.techjuice.pk/bank-biometric-verification-last-date/ , 2019.