# USERS' OPINION REGARDING COMPARISON BETWEEN SINGLE-FACTOR AND TWO-FACTOR AUTHENTICATION USING PARAMETERS OF SECURITY AND USABILITY IN SOCIAL MEDIA APPLICATION

Ghulam Mustafa Khaskheli*, Marina Sherbaz, Umair Ramzan Shaikh

Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Nawabshah, Pakistan

*Corresponding E-mail: ghulammustafa@sbbusba.edu.pk

**ABSTRACT**

**Objective:** Main objective of this research is Users' point of view in comparison of single-factor with two-factor authentication utilizing parameters of security and usability in social media application.

**Research Method:** In this research study, an experiment was conducted to describe the users' perceptions towards comparison of single-factor and two-factor authentication methods on a social media application with usability and security utilizing three One-Time Password generator software on mobile phone. The research took place with 50 social media users. First single factor authentication procedure was performed followed by Two Factor Authentication process. The data were gathered through 7-point Likert scale using a questionnaire for testing the usability. Comparison was done between single factor with two-factor authentication approach.

**Findings:** The responses were compared through t-test using Statistical Package for the Social Sciences version 21. There was statistically significant difference between both authentication methods. According to the results, two-factor authentication method is more secure than single-factor authentication.

**Originality:** Beside it, this approach was having less perception of usability and lesser evaluations for comfort and convenience for the two-factor variant. Likewise, the two component validation form took more time for members to finish. This examination gives important experimental proof of the compromise among security and ease of use in computerized frameworks.

**Keywords:** software security, single factor, two factor authentication

## 1. INTRODUCTION

Programming security is a process carried out to safeguard applications against noxious attack and other applications chances so the application keeps on working properly under such likely threats. Security is compulsory for uprightness, verification and accessibility. The most common way of recognizing clients that solicitation is Authentication which is admittance to a framework, organization, or gadget.

Cybercriminals generally work on their assaults. Therefore, security groups are confronting a lot of verification related difficulties. For this reason organizations are beginning to carry out more modern occurrence reaction systems, including confirmation as a feature of the interaction. Some normal verification techniques used to get present day frameworks are.

### 1.1 PASSWORD AUTHENTICATION

The most common stratigies for authentications are Passwords and it can be letters in series, numbers, or exceptional characters. To protect yourself you need to make strong passwords that fuse a mix of every single decision.

### 1.2 MULTI FACTOR AUTHENTICATION

It is a validation technique in which two ways of recognizing a client are followed. Models incorporate codes created from the client's advanced mobile phone, Captcha tests, fingerprints, or facial acknowledgment.

### 1.3 CERTIFICATE BASED AUTHENTICATION

Certificate-based authentication innovations recognize clients, machines or gadgets by utilizing computerized endorsements. A computerized declaration is an electronic record in light of the possibility of a driver's permit or a visa.

### 1.4 BIOMETRIC AUTHENTICATION

**B**iometrics authentication is a security process that relies on the unique biological characteristics of an individual.

### 1.5 SERVICE PROVIDER

A service provider is an individual or entity that provides services to another party. It also can be an association which gives Information Technology support administrations to inner and outside clients.

Service Providers are divided in three types

- Internal service provider (one): An organization to deliver services of Information Technology .
- Shared service provider (two): this type of service providers provides IT services to more than one units within the industry.
- External service provider (Three): in this type services of Information Technology are provided to outside customer of any organization.

### 1.6 FACEBOOK

facebook is a site which permits clients, who pursue free profiles, to interface with companions, work partners or individuals they don't have the foggiest idea, on the web. It permits clients to share pictures, music, recordings, and articles, as well as their own contemplations and suppositions with anyway many individuals they like.

### 1.7 DROPBOX

Dropbox would one say one is of a few well known distributed storage benefits that empower you to store and share your records on the web "in the cloud." What does that mean? It implies that you can store and back up your records online for simple access from anyplace - your home PC, your work PC, or your cell phone. Your records are put away on Dropbox's servers and can be synchronized, or naturally stayed up with the latest, on the entirety of your gadgets. The fundamental Dropbox administration is free, yet you can redesign for an expense to get more extra room and extra elements.

### 1.8 AMAZON

Amazon.com is an enormous Internet-based undertaking that sells books, music, movies, housewares, equipment, toys, and various different product, either directly or as the intermediary between various retailers and Amazon.com's colossal number of clients. Its Web organizations business joins renting data accumulating and enlisting resources, claimed "dispersed registering," over the Internet. Its critical electronic presence is with the ultimate objective that, in 2012, 1 percent of all Internet traffic in North America went all through Amazon.com server ranches.

### 1.9 OTP APPLICATIONS

A one-time password (OTP) is a consequently created numeric or alphanumeric series of characters that verifies the client for a solitary exchange or login meeting.

An OTP is safer than a static secret word, particularly a client made secret key, which can be feeble as well as reused across different records. OTPs might supplant confirmation login data or might be utilized notwithstanding it to add one more layer of safety.

### 1.10 AEGIS AUTHENTICATOR

Aegis Authenticator is a free, secure and open source application to deal with your 2-venture check tokens for your internet based administrations. Aegis upholds the (**HMAC-based One-Time Password**) HOTP and (**time-based one-time password**) TOTP calculations. These two calculations are industry-standard and broadly upheld, making Aegis viable with huge number of administrations.

### 1.11 GOOGLE AUTHENTICATOR

Google Authenticator creates double Step Verification codes on your phone. 2-Step Verification gives more grounded security to your Google Account by requiring a second step of confirmation when you sign in. Notwithstanding your secret key, you'll likewise require a code created by the Google Authenticator application on your telephone.

### 1.12 MICROSOFT AUTHENTICATOR

Microsoft Authenticator is a multifaceted application for cell phones that produces time sensitive codes utilized during the Two-Step Verification process.

Security has been a big question for large service providers, including Google, Facebook, Amazon and others to answer the question so many methods have been implemented one of them is two factor authentication(2FA), it is a technique for accessing an online account that needs the user to provide two different types of information

## 2. LITERATURE REVIEW

ALSaleem & Alshoshan (2021) studied a multi-factor authentication system that combines the ease of use and the low-cost factors is proposed. The system did not need any special settings or infrastructure. It was designed depending on graphical passwords. The proposed system might overcome many different security threats, such as key-loggers, screen capture attack or shoulder surfing. The proposed method was applied to 170 participants, 75% of them are males and 25% are females, classified by age group, education level, web experience, where one-third of them do not have sufficient knowledge about various security threats. he proposed system was created to protect the user's data in a way that no program can catch the user passwords or even the authentication methods he uses.

Chishti et al (2021) proposed a methodology for efficient communication between active NFC devices using NFC read/write mode. To evaluate the scheme, we design a secure Multi-Factor Authentication (MFA) system that requires bi-directional communication for mutually authenticating two NFC devices. The proposed methodology is experimentally verified using NFC-enabled Android smartphones and a Kerberos server as the third-party authenticator.

Ozkan & Bicakci (2020) after analyzing eleven different Android authenticator applications reported that we report that we have fetched cleartext shared secret seed value from storage in five applications and from memory in seven applications using standard reverse engineering techniques and open-source tools. Future work may include developing a tool that takes heap dump of every consecutive second.

Alamsyah et al (2020) study aimed to strengthen the scheme by combining RSA with the One Time Pad algorithm so that it will bring up a new design to be used to enhance security on two-factor authentication. Contribution in this paper is to find a new scheme algorithm for an enhanced scheme of RSA. One Time Pad and RSA can combine as well.

Gordin et al (2019) dealt with two factor authentication at both the user interface level (Horizon component) and the authentication level (Keystone component). For each user in the cloud, a TOTP account is created to which a 16-character secret password is assigned randomly. The secret password is then converted to base format 32. To eliminate errors that may occur when the user transcribes the code, in line with similar trends used by other applications, we have opted to convert the password into the QR image and send it by email. The user uses a smartphone application that allows the secret password to be converted into unique code (eg. Google Authenticator). One downside of this type of authentication is represented by increased complexity of authentication. The unique code input field requires a little more time for the user to be completed and his mobile device to be setup accordingly.

Reimair et al (2016) proposed work is complementing U2F by the distinct features of CrySIL. CrySIL allows for upgrading existing (crypto-capable) devices to U2F authenticator devices while keeping the physical efforts minimal for the user. We demonstrated our approach by enabling U2F login to websites and Microsoft Windows 10 with devices such as cryptographic smart cards, Austria's eID, cloud key services and smartphones. The evaluation showed that our enhancements benefit the usability and convenience of U2F while keeping security properties intact. All in all, we believe that our contribution can push acceptance of U2F even further and thus, make everyone benefit from state-of-the-art authentication.

Joshi et al (2012) proposed an idea to recover soldier surfing attack using certificate generation scheme. In this purposed mechanism server will generate a verification code inside the certificate in which server will send on user mail id or on mobile phone if provided along with the certificate (not to the phone ) this verification code will be unique to the user. This type of authentication finds usage on military operation, large data base server, nuclear plant and missile operation etc. For future purpose small 3D virtual environment authentication can also implement on operating system's login and ATM security.

O'Gorman (2003) proposed authenticators by three types according to how they provide security: knowledge-based, object-based, and ID-based. A knowledge-based authenticator provides security by secrecy, and examples are a combination lock and a password. A object-based authenticator provides security by being closely held, and examples are a metal key and an ATM card. An ID-based authenticator provides security by uniqueness and copy-resistance, and examples include a passport and a biometric. We compare authenticators with respect to potential attacks and other issues. The attacks include client and host search attacks, eavesdropping, theft (including biometric forging), replay, Trojan horse, and denial of service. Other security issues include non repudiation, compromise detection, and the administrative issues of registration/enrollment, reset or compromise recovery, and revocation. Although an appropriate authentication solution depends upon the particular application, a few combinations of authenticators are recommended.

## 3. DATA COLLECTION

Data of 50 social media users was gathered through likert format questionnaire, first using single factor authentication procedure and than by 2FA authentication process, common questions for testing usability were targeted, data of both single factor and 2 factor was compared.

Furthermore to implement two factor authentication by third party application an OTP generating free application from Google app store was install on Smartphone, three applications usability was targeted Aegis, Google Authenticator and Microsoft Authenticator to find out which applications is efficient in terms of usability.

Basic differentiations were found between the two strategies, with the two-factor rendition being seen as offering more elevated levels of safety than the single-factor validation variant; notwithstanding, this gain was balanced by altogether lower view of ease of use, and lower appraisals for comfort and usability for the two-factor adaptation.

### 3.1 APPLICATION USEFULNESS OF AEGIS, MICROSOFT AND GOOGLE AUTHENTICATOR

In Figure 1uselfulness of three authenticators (Aegis, Microsoft and Google) is checked by utilizing 7 points likert scale.

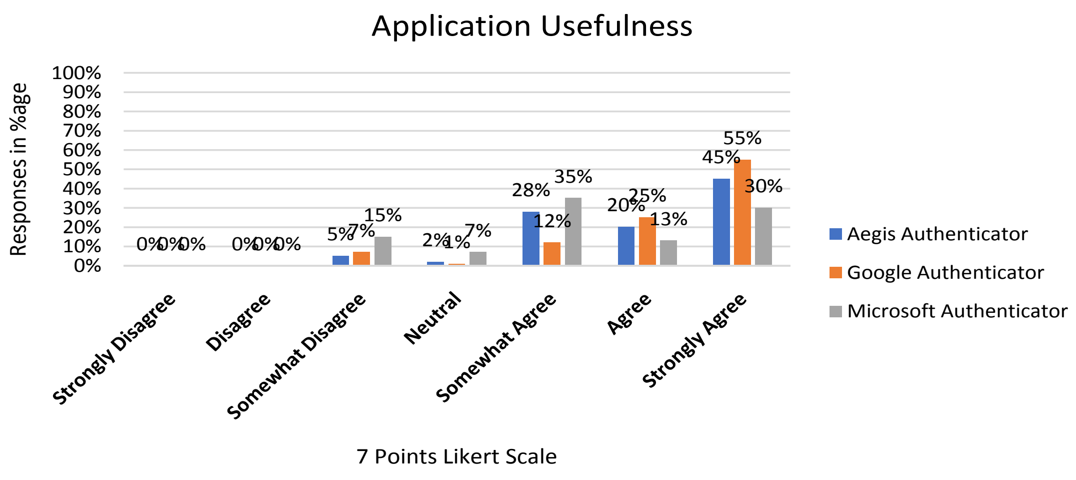

**Figure 1:** Application usefulness of Aegis, Microsoft and Google authenticator

### 3.2 APPLICATION EASE OF USE OF AEGIS, MICROSOFT AND GOOGLE AUTHENTICATOR

In Figure 2 Ease of use of three authenticators (Aegis, Microsoft and Google) is calculated checked by utilizing 7 points likert scale

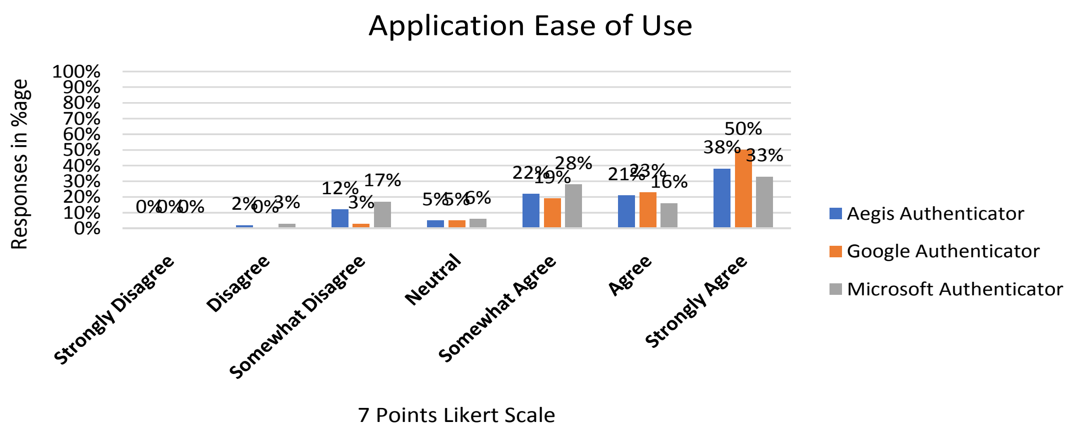

**Figure 2:** Application Ease of Use of Aegis, Microsoft and Google authenticator

### 3.3 APPLICATION EASE OF LEARNING OF AEGIS, MICROSOFT AND GOOGLE AUTHENTICATOR

In Figure 3 Ease of use of three authenticators (Aegis, Microsoft and Google) is calculated checked by utilizing 7 points likert scale.

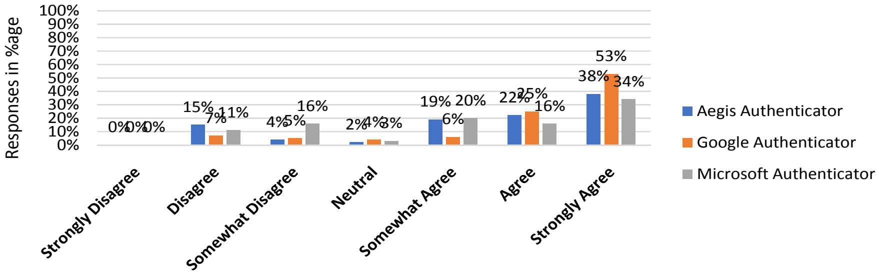

**Figure 3:** Application Ease of Learning of Aegis, Microsoft and Google authenticator

## 3.4 APPLICATION SATISFACTION OF AEGIS, MICROSOFT AND GOOGLE AUTHENTICATOR

In Figure 4 Ease of use of three authenticators (Aegis, Microsoft and Google) is calculated checked by utilizing 7 points likert scale.

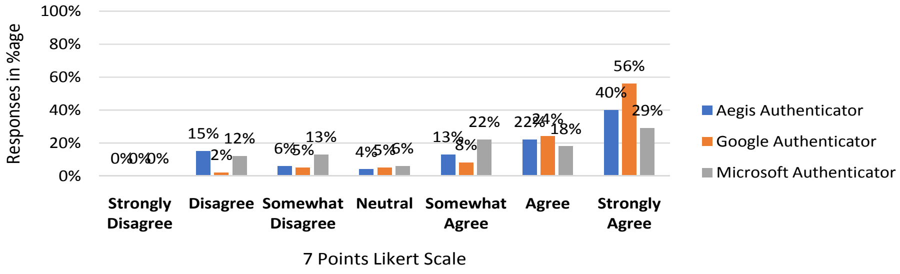

**Figure 4:** Application Satisfaction of Aegis, Microsoft and Google authenticator

## 3.5 OVERALL APPLICATION FEATURES AND SURVEY RESULTS

In Figure 5 overall application features and survey results are discussed

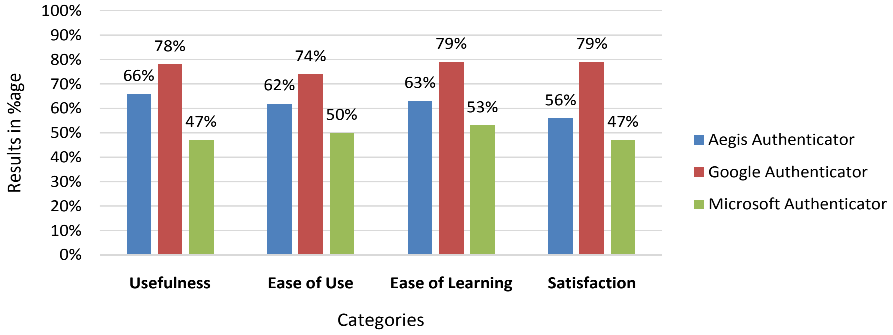

**Figure 5:** Overall Application Features and Survey Results of Aegis, Microsoft and Google authenticator

## 4. RESEARCH METHODOLOGY

Usability engineering works on enhancing the usability of interactive systems. It draws on assumption from computer science and psychology to define issues that occur during the use of such a system. The examination approach utilized in this exploration includes a contrastive report where two renditions of the exchange framework, varying in some plan trademark, are capable by members in a research facility setting. Members are given nitty gritty individual information as made up personae to use during the analysis and are approached to perform assignments run of the mill of genuine use inside the discourse framework. The outcomes acquired from this strategy are considered to inexact the reactions the assistance would create in a true setting of utilization.

A rich arrangement of information is gathered in light of execution estimations, (for example, time taken to follow through with jobs and achievement rates) and abstract perspectives to the encounters of utilizing the various renditions of the assistance. During the investigation, specialists mention direct observable facts about the conduct of the members; these give important bits of knowledge into the non-verbal responses of members utilizing the intelligent frameworks.

Members' perspectives are estimated utilizing polls finished subsequent to encountering every variant of the assistance. The survey utilizes a Likert design (Likert, 1932) where every convenience property to be estimated is introduced to the member as an upgrade proclamation followed by a concur differ scale. The upsides of this arrangement have been portrayed (Coolican, 1990) as:

- Members lean toward the Likert scaling procedure since it is "more normal" to finish and on the grounds that it keeps up with their immediate association simultaneously.
- The Likert method has been displayed to have a serious level of legitimacy and unwavering quality.
- The Likert scale has been demonstrated to be viable in estimating changes after some time.

A usability questionnaire in Likert format has been constructed to measure these attributes. The Questionnaire covers cognitive issues (e.g. level of concentration required by users, and how stressful the service was to use), the fluency and transparency of the system (e.g. ease of use and degree of complication), system performance (e.g. the efficiency of the application and users' preferences for a human agent).

The 7 point Likert scales are utilized with equilibrium of decidedly and contrarily phrased upgrade explanations in the poll. On this scale, when the reactions are standardized for proclamation extremity, a score over 4.0 addresses an uplifting outlook; scores beneath 4.0 address negative perspectives to the distinguished qualities, and every member's general disposition to the assistance can be estimated by taking the mean of these numbers across every one of the things in the survey.

A proportion of the general demeanor to the assistance can then be gotten by averaging all the survey results for members who encountered that help. Whenever answers to emotional survey credits are assembled from numerous clients thusly, the normal outcomes can be viewed as a true proportion of framework claim. Additionally, when scores are gathered for a long time renditions of a framework plan, these can measure up and used to figure out which is generally fulfilling to utilize. Authentication approaches compared as:

- Two ways to deal with client confirmation were thought about in the trial.
- The single-factor approach depends on a "what you know" strategy.
- The two-factor approach inspected in the investigation contains an extra "what you have" part. Different OTP creating applications are right now accessible for use in improved security.

Three types of OTP generator with pros and cons for each, In this research, OTP application as two actor authentication was used- OTP Generator is a virtual device application for multi-factor authentication (MFA), so-called two-step verification, which generates time-based one-time passwords (OTP).

When a user tries to login on social media account after registering through OTP generator application a unique one-time six to eight-digit access codes is shown on the application. In the system investigated in the experiment, the user inputs (all of) this one-time access code in application to login. Three different OTP generator were used by all 50 users one by one, This application doesn't consider the chance of being lost or taken, is clearly install on Smartphone of social media user. It is, however, recognized that the extra security presented by such a methodology is just of advantage if clients uses the OTP generator also comprehend its worth; subsequently the inspiration for this exploration.

Fifty social media users took part in the experiment, in a design that was approximately balanced for age and gender. All were using same social media application involved in the study. Equal numbers of participants from each gender were recruited, 25 males, 25 females.

The investigation approach utilized in this examination includes a contrastive report where two variants of the exchange framework, varying in some plan trademark, are capable by members in a lab setting. Members are given nitty gritty individual information as made up personae to use during the test and are approached to perform assignments ordinary of genuine use inside the exchange framework. The outcomes acquired from this methodology are considered too rough the reactions the assistance would create in a true setting of utilization.

First social media user login to their respective account using single factor authentication than they attempt a questionnaire with likert scale format having seven options for each question ranging from strongly disagree to strongly agree. Secondly user tries to login through two factor authentication technique, user register their social media account with OTP generator application and attempts to login, during the process behavior of user is recorded to find out how much system is usable.

After that three OTP generator applications are selected from google app store to find out which application is more usable, Three applications(Aegis authenticator, Google authenticator and Microsoft authenticator) are involved in experiment as well to compare the features and usability of all three applications, use questionnaire was used to find out the usability of all three OTP generator application to find out the usability in four different areas.

## 5. RESULTS AND DISCUSSIONS

The timings for each participant for each version were recorded with the single factor authentication version followed by two factor authentication version.First data of single factor authentication was compared with the data of two factor authentication. The overall mean completion timing for the single-factor version on a social media application was 7.795 seconds, and for the two-factor was 34.578 seconds.

The outcomes showed that the contrast between variants was exceptionally huge. Be that as it may, this is true to form since the two-factor way to deal with validation doesn't supplant the single-factor approach however rather adds an extra stage to it. Consequently the spans for ID and check of the two-factor form would be relied upon to be longer.

A significant interaction of two factor authentication version with three different OTP generators was also found. When experienced first OTP application (Aegis authenticator) with social media, it took an average of 37.734 seconds; when experienced second OTP application (Google authenticator) with social media the mean time for this version was just less than 32 seconds. While in third OTP application (Microsoft authenticator) with social media the mean time for this version was 34.57seconds.

Considering that the two-factor approach consolidates the single-factor methodology this isn't completely is to be expected; it does, in any case, outline the significance of adjusting the request where members experience the two unique variants to get a genuine measure of the mean validation term for each situation. The mean usability scores derived from the usability questionnaires of each user was not more than 5 (on a 7-point scale) for the single-factor version and overall means score for all user was 4.15 for the single-factor version. The mean usability scores derived from the usability questionnaires of each user was near 5 (on a 7-point scale) for the two factor version and overall average score for all user was 5.

The usability of the single-factor authentication method was judged to be significantly higher than the two-factor access device version. In addition, the interaction between the usability of each service and the order of experience indicated a moderately significant effect. Participants in both order groups rated the single-factor version higher than the two factor version.

Table 1.1 defines the comparison among the OTP authenticator applications; three applications Aegis authenticator, Microsoft authenticator and Google authenticator were compared to relate the features of all three applications.

**Table 1:** Features comparison of Aegis, Microsoft and Google authenticator

| Aegis Authenticator | Microsoft Authenticator | Google Authenticator |
|---|---|---|
| Aegis Authenticator is a free, secure and open source application to deal with your 2-Way confirmation tokens for your web-based administrations.<br>Compatibility<br>Aegis upholds the HOTP and TOTP calculations. These two calculations are industry-standard and generally upheld, making Aegis viable with large number of administrations. Any web administration that supports Google Authenticator will likewise work with Aegis Authenticator. | 2FA is simple, helpful, and secure when you use Microsoft Authenticator. Utilize your telephone, not your secret word, to sign into your Microsoft account. Simply enter your username, then, at that point, support the warning shipped off your telephone. Your finger impression, face ID, or PIN will give a second layer of safety in this two stage check process. After you've endorsed in with two element confirmation (2FA), you'll approach all your Microsoft items and administrations, like Outlook, OneDrive, Office, and that's only the tip of the iceberg. | Google Authenticator generates 2-Step Verification codes on your phone.<br>2-Step Verification provides stronger security for your Google Account by requiring a second step of verification when you sign in. In addition to your password, you'll also need a code generated by the Google Authenticator app on your phone. |
| Feature overview<br>• Free and open source<br>• Secure<br>• Encrypted, can be unlocked with a password or biometrics<br>• Screen capture prevention<br>• Tap to reveal<br>• Compatible with Google Authenticator<br>• Supports industry standard algorithms: HOTP | Microsoft Authenticator additionally upholds multifaceted validation (MFA) regardless of whether you actually utilize a secret word, by giving a second layer of safety after you type your secret key. While signing in with two variable verification (2FA), you'll enter your secret word, and afterward you'll be | Features:<br>* Generate verification codes without a data connection<br>* Google Authenticator works with many providers & accounts<br>* Dark theme available<br>* Automatic setup via QR code<br>* Transfer accounts between devices via QR |

| | | |
|---|---|---|
| and TOTP<br>• Lots of ways to add new entries<br>• Scan a QR code or an image of one<br>• Enter details manually<br>• Import from other popular authenticator apps<br>• Organization<br>• Alphabetic/custom sorting<br>• Custom or automatically generated icons<br>• Group entries together<br>• Advanced entry editing<br>• Search by name/issuer<br>• Material design with multiple themes: Light, Dark, AMOLED<br>• Export (plaintext or encrypted)<br>• Automatic backups of the vault to a location of your choosing<br><br>Open source and license Aegis Authenticator is open source and licensed under GPLv3. The source code is available here: https://github.com/beemdevelopm | requested an extra method for demonstrating it's truly you. Either endorse the notice shipped off the Microsoft Authenticator, or enter the one time secret word (OTP) created by the app. The one time passwords (OTP codes) have a 30 second clock counting down. This clock is so you never need to utilize a similar time based one time secret key (TOTP) two times and you don't need to recollect the number. The one time secret key (OTP) doesn't expect you to be associated with an organization, and it won't deplete your battery. | code<br><br>Permission notice: Camera: Needed to add accounts using QR codes |

## 6. CONCLUSIONS

This experiment explored user attitudes towards the usability and security of single-factor and two-factor methods for authentication on a social media application. The results show some interesting differences between the two authentication approaches. In terms of performance, unsurprisingly the two-factor process involving an additional stage took significantly longer to complete than the single-factor method. Both approaches to customer authentication obtained a mean usability rating near 5.0 on the 7-point scale, indicating a generally positive reaction to the services (5.56 for the single-factor version and 5.31 for the two-factor version).

There was, however, significant evidence that the singlefactor knowledge-based authentication process was more usable than the two-factor process employing an additional one-time access code from an OTP generator application. The single-factor approach was rated (moderately) significantly higher overall, and for seven of the twenty-two usability attributes measured in the experiment. The twofactor version, in contrast, scored significantly higher only on the issue of security. Overall ratings for ease of use, convenience and security exhibited a similar pattern, with the single-factor approach considered significantly easier to use and more convenient than the two-factor version, but less secure.

From a practical point of view these data are likely to be a comfort to those considering use of a similar (two-factor token-based) approach to authentication. Although the gain in security obtained through such an approach is associated with a decrease in the usability of the service it could be argued that the effect is relatively moderate, given users' (lack of) overall preference and the positive usability score awarded to the two-factor version.

## REFERENCES

Alamsyah, Z., Mantoro, T., Adityawarman, U., & Ayu, M. A. (2020). Combination RSA with One Time Pad for Enhanced Scheme of Two-Factor Authentication. In 2020 6th International Conference on Computing Engineering and Design (ICCED), IEEE, 1-5.

ALSaleem, B. O., & Alshoshan, A. I. (2021). Multi-Factor Authentication to Systems Login. In 2021 National Computing Colleges Conference (NCCC), IEEE, 1-4.

Chishti, M. S., King, C. T., & Banerjee, A. (2021). Exploring half-duplex communication of NFC read/write mode for secure multi-factor authentication. IEEE Access, 9, 6344-6357.

Gordin, I., Graur, A., & Potorac, A. (2019). Two-factor authentication framework for private cloud. In 2019 23rd International Conference on System Theory, Control and Computing (ICSTCC) IEEE, 255-259.

Joshi, A., Kumar, S., & Goudar, R. H. (2012). A more multifactor secure authentication scheme based on graphical authentication. In 2012 International Conference on Advances in Computing and Communications, IEEE, 186-189.

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040.

Ozkan, C., & Bicakci, K. (2020). Security Analysis of Mobile Authenticator Applications. In 2020 International Conference on Information Security and Cryptology (ISCTURKEY), IEEE, 18-30.

Reimair, F., Kollmann, C., & Marsalek, A. (2016). Emulating U2F authenticator devices. In 2016 IEEE Conference on Communications and Network Security (CNS), IEEE, 543-551.