FIT2093 Introduction to Cyber Security
Assignment 1: Investigating an Application of Cryptography

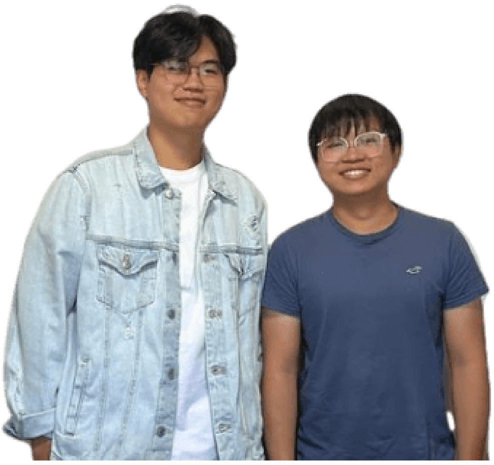
Topic: Multi-factor Authentication Systems

Team Broccoli

Lim Zheng Haur (32023952)
Yap Jit Feng (32898339)

Number of team members: 2

Team Photo:



-

Introduction:

In today's society, digitalisation in every aspect of life is considered to be a necessity. As we can do anything with just a singular device on our hands. There are a total of 5.1 billion internet users around the world and 92% of them are using the internet through their mobile devices (Richardat, 2023). The total internet users are increasing exponentially but most of them are not aware of the risk of their internet security being exploited. This is because they do not know about the danger of attackers impersonating them to steal their data. This type of attack is called an impersonation attack. This type of attack is mainly targeting the user's confidentiality and authentication on the server. One of the most well known security systems to counteract this attack is called the Multi-factor authentication system.

Multi-factor authentication systems are a type of security system that prevents unauthorised individuals/users from accessing private information. Multi-factor authentication prevents attackers from accessing with only the victim's password. This is because a multi-factor would need a combination of different forms of information from the user (Williamson & Curran, 2021). There are 3 different forms of information which are physical information, intelligence based information and inherited information. Physical information are essentially mobile devices, laptops, desktop computers and any other physical devices the user owns. Intelligence based information is data created by the user when opening an account such as passwords, individual answers, personal keys and many more. Inherited information is unique towards different individuals because those are data which are located on the users itself. This information includes facial features, eye colour, thumbprints, etc.

The main security goal for multi-factor authentication is to protect user's authentication and confidentiality. This means that it reduces the chance of accounts being compromised by third parties individuals while strengthening the security of the user's account (Kim & Hong, 2011). Multi-factor authentication protects user's authentication by making users provide 3 forms of identification and would have to undergo different steps in order to access their database/services. Even Though the security is high, the usability for the users is bad. This is because it is a hassle for users to go through all the steps of authentication every time when they log into their account.

There are multiple different types of journal articles that are used in this report. There are journals that analyses the strengths and weaknesses of multi factor authentication systems. Journal articles that provided their own improvements to the system were also reviewed in this report. Usability and performance results were displayed via screenshots to be further discussed. All the main journal articles used were also listed in the following:

- A method of risk assessment for multi-factor authentication by Kim & Hong (2011).
- A comparative usability study of two factor authentication by Christofaro et al (2014).
- Design and implementation of cost effective mult-factor authentication framework for ATM systems by Abiew et al (2020).
- User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking by Gunson et al (2011).

- Users opinion regarding comparison between single-factor and two factor authentication using parameters of security and usability in social media application by Khaskheli et al (2022).
- Evaluating the usability of two-factor authentication by Reese et al (2018).

Throughout the journal, it began by introducing the different types of multi-factor authentication while explaining advantages and disadvantages for them. Multi-factor authentication cryptography methods and techniques will be analysed in detail. The main threats and attacks that the security system is made for will be discussed. The performance and usability of the multi factor authentication system will be analysed and compared based on results from other research papers provided above. Furthermore, vulnerabilities on multi factor authentication will be provided to improve the future of the security system. Comparison between different authentication apps will be analysed to display the best combination of authentication results. Finally, a conclusion will summarise all the main topics and a recommendation on future improvements will be listed.

Application Protocol/System

Multi-factor authentication is a security that asks for multiple different types of information when logging in to their accounts. This is to protect users from imposters impersonating them to steal their information. In order to activate multi-factor authentication, users must undergo multiple steps of validation. These steps are required to maintain the user’s confidentiality and authenticity. Users' authentication are broken into 3 separate groups which are information that the user knows, information that can be held physically and information that they inherited from their parents. These individualised authentication are also known as single factor authentication which is the simplest form of multi factor authentication (Gunson et al., 2011). The main advantage of the single factor authentication is that its usability is the best amongst the rest. This is because users would only need to provide one information such as a password, biometric or face recognition to access their data. Furthermore, it is the cheapest form of multi-factor authentication as they require less hardware/software to support it. Single-factor authentication. However, it is easy to break the security system when the attacker acquires the users’ one of the 3 authentications.

The most common single factor authentication is information that the user knows/created. These information are password, personal identification number, personal answers and many more. Knowledge factors are the most important part in every multifactor authentication. This is because it is the main defence for every security system known (Reno, 2013). Passwords and personal answers are used in every website when requesting users to create an account, while PIN can be found on every card transaction. Physical factor authentication are basically physical items that identify the users such as identity card, credit card, mobile phone and many more. Most companies use a physical factor to send a randomly generated number to prove the user’s authenticity. Finally, inherited factor authentication uses an individual's facial features and biometrics to determine their identity. These can be found on most smartphones/devices where they will scan for biometrics or facial features for quick access.

There are also some cases where companies scan for similar voice frequencies or eye geometry to access classified data (Reno, 2013).

Another form of multi-factor authentication is two-factor authentication. Two-factor authentication is basically instead of one authentication, it will need 2 out of the 3 authentication. It is not the strongest form of multi-factor but it is significantly better than single factor. Attackers will need to acquire two different sets of information in order to access the user's data. The most common two factor authentication is the combination of PIN number and a one time password(OTP) sent to users mobile phone. This time of two factor authentication is called TOPT authentication. Apps such as microsoft authenticator, okta authenticator and google authentication uses two factor authentication as their main security. Even though they use the same security system, their encryption algorithms are different. On these apps, new OTP are generated randomly for a short period of time. This is to ensure attackers can’t use the same OTP to access the user's account. Besides that, users will receive a notification when an external party tries to enter their account without permission. The other forms of multi factor authentication needs users to provide 3 or more different forms of authentication. It is basically two factor authentication that includes using users facial features or biometrics. This is the strongest form of authentication as an attacker would not be able to access users data with just password and an OTP.

In Multifactor authentication, encryption technology is not used in the main authentication system. However, it is normally used to transfer information and protect authentication information. The main encryption method used in multifactor authentication is RSA encryption which is also asymmetric encryption (Ali et al. 2020; Kim & Hong, 2011). The RSA encryption system encrypts messages using a public key and turns it into a ciphertext. This public key is given out openly meaning that anyone can use the public key whenever they want. However, to decrypt the ciphertext users would need to acquire a private key provided to them secretly. RSA encryption uses prime number and modular functions as their main encryption defence. This method of encryption is difficult to decrypt because it takes a long time to perform modularization to a large prime number. Besides that, the double hash function is also used to hide secret numbers (Ali et al. 2020; Kim & Hong, 2011). Double hash function is essentially performing hashing on a number twice which means that the secret number will be scrambled twice. Since hashing is a one way operation, it is one of the best ways to hide data from attackers. Symmetric encryptions are also used in multifactor authentication systems (Ali et al. 2020; Adeyemo, 2015). Symmetric encryption is similar to asymmetric encryption but it only uses one single key to encrypt and decrypt the data. Symmetric have multiple different ways for sharing keys but the most common one is called the diffie hellman key exchange algorithm. Diffie hellman key exchange involves both parties to select a random number and perform mathematical operations to get a base number. This base number will be exchanged with one another to perform mathematical operations again to get a final private key. This private key will be used to encrypt and decrypt the data. This symmetric encryption is hard to penetrate because it is difficult to compute a key with large prime numbers which is impossible.

Multi Factor authentication is always used in big companies to protect the consumer authentication. It can be found when users create a new account on a website such as facebook, gmail, microsoft account and many more. Normally, third party authentication systems are used by most companies but big companies like Microsoft develop their own multifactor authentication system. Microsoft authentication system uses two factor authentication where they will first ask users to input their credentials to create an account. Then Microsoft will suggest users to download their authentication app to improve protection towards their account. The app will make the current smartphone as a physical authentication for the user. This means that the verification process can only be done on the phone, but users will have a choice to transfer the authentication information to another phone. After the registration process, User will have to go through the initial login phase with the multi factor authentication process. When users key in their account credentials, they will be alerted to go to the authentication app to confirm their actions. If users select yes, they will be provided a OTP that will verify their identity.

Different amounts of authentications will have different security levels. Single factor authentication has the lowest security level compared to the rest. This is because if an attacker has access to one of the authentication information, then they will have full access to users data. Since it is the lowest level of security, single factor authentication can only protect users vulnerable to most attacks such as replay attack, man in the middle attack, brute force attack and many more.

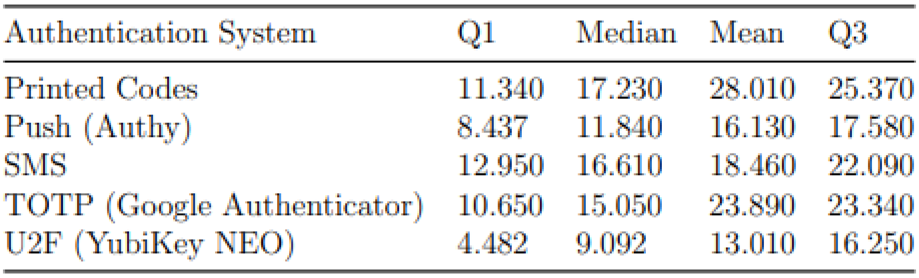
Two Factor authentication is a security system that is better than single factor by a wide margin. This is because of having 2 different combinations of authentication. It can protect users from attacks such as brute force attack, online guessing, replay attack, eavesdroppers and many more (Abiew et al, 2020; Ali et al, 2020; Kim & Hong, 2011). Two factor authentication prevents brute force attack, by having a second authentication information such as OTP number or fingerprint. This will prevent hackers from accessing users' accounts with only a password. Any attacks that rely on one of the user credentials will be useless against the security system. Since most of the two authentication systems will have different types of encryption algorithms to transfer information from users to the database (Adeyemo, 2015). This will prevent eavesdropping attacks by having the communication encrypted via hash encryption, symmetric and asymmetric encryptions. It will take a long time for the attacker to decrypt the ciphertext as they will need to determine a key generated using large prime numbers. By the time they found the key, the algorithm had already changed the private key for both of the parties constantly.

Multi Factor authentication that needs all 3 of the authentication methods is the strongest amongst the rest. It can prevent the attacks that single factor and two factor designed to do but better. Multi Factor authentication can prevent man in the middle by having an inherited authentication as another level of security system (Ali et al, 2020). Man in the middle attack intercepts communication between two parties to gain personal knowledge which include users knowledge authentication and OTP (Yasar & Cobb, 2022). If attackers have the user's password/PIN and their mobile devices, they will still need users' biometrics to gain access to their account. Multifactor authentication also contains encryption algorithms to encrypt communications between the users and their database (Ali et al. 2020). Encryption algorithms like symmetry encryption are one of the best defences against man in the middle attacks. Multifactor authentication systems are also good against spoofing attacks. Spoofing attack is a type of attack that tricks users into using their services by pretending to be legitimate websites (Folger, 2022). This will help attackers in acquiring multiple different type information such as IP address, PIN number, credit card information and many more. Multifactor authentication systems help users by enforcing an inherited authentication where attackers can't access their data without their biometrics.

Application Protocol/System Performance & Usability Results

Multi Factor authentication has different performance and usability results. This is because the implementation for each authentication method is different between each other. For example, single factor authentication has the highest usability but with a lower performance result because users would only have to key in their username and password to access their data. On the other hand, two factor authentication has the lower usability factor but higher performance because users have to go through two different authentication methods in order to access their information. The results gained from journal articles have been used to further analyse the performance and usability of multiple different forms of multi factor authentication.

Table 1: Authentication Time (in Seconds), Summary Statistics

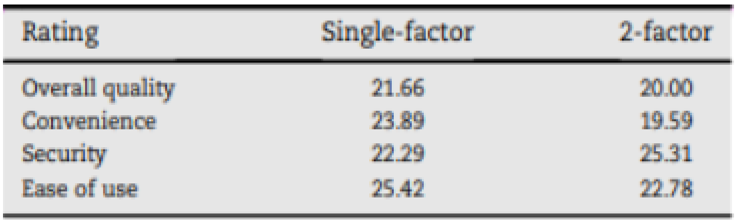


Authentication System	Q1	Median	Mean	Q3
Printed Codes	11.340	17.230	28.010	25.370
Push (Authy)	8.437	11.840	16.130	17.580
SMS	12.950	16.610	18.460	22.090
TOTP (Google Authenticator)	10.650	15.050	23.890	23.340
U2F (YubiKey NEO)	4.482	9.092	13.010	16.250

Authentication Time(in Seconds), Summary Statistics by Reese, K. R., Seamons, K., Zappala, D., & Ventura, D. 2018

In table 1, it demonstrates the speed performances of different two factor authentications. There are 5 different combinations of intelligence authentication and physical authentication. This means that the authentications will ask the user for their pin/password and an OTP to access their services. The authentication systems are measured using the time taken users receive a push notification when they enter their password. According to the table, the fastest two factor authentication is U2F key, while Printed Code is the slowest. U2F authentication is a type of two factor authentication that allows users to create a physical authentication using a USB (Garska, 2018). To authenticate the users, users will always need the USB to access their database. U2F authentication is quick because the authentication system will approve once they detected the usb (with the key)in the computer. Printed Code is the slowest as users would need to wait for the code to be printed via printer, thus making the process very tedious. On the other hand, SMS authentication systems are the second slowest because they rely on a user's phone number to receive a randomly generated OTP. Users then will need to key in the OTP into the authentication security system to access their data. It is because the speed of the OTP request is determined by the cellular signal (Reese et al, 2018). This means that the slower the cellular signal, the slower the OTP being received. Overall, the average speed performance of all the two factor authentications is around 20 seconds.

Table 2: Ratings for two authentication method

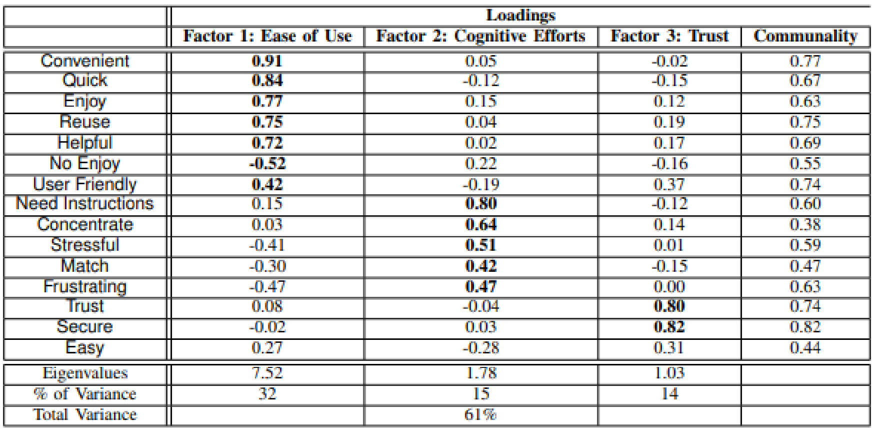


Rating	Single-factor	2-factor
Overall quality	21.66	20.00
Convenience	23.89	19.59
Security	22.29	25.31
Ease of use	25.42	22.78

Ratings for the two authentication methods by Gunson, N., Marshall, D., Morton, H., & Jack, M. 2011

The table 2 above demonstrates a rating statistic comparison between single factor and two factor authentications. The table shows that the overall quality of single factor authentication is 1.66 better than two factor authentication. This is because the convenience and ease of use rating is greater than two factors . On the other hand, the security rating for 2 factors is greater by 3.01. Single factor authentication has a higher overall rating than 2 factor because users would only need to key in their credentials to gain access to their data. This limits the security aspect of single factor, as attackers/intruders can just log in users' accounts with stolen username and password. This results in 2 factor authentication to have a higher security rating since users would need 2 different types of authentication to gain access to their account. This means that an attacker couldnt access users data with just intelligence based authentication. Even though the security factor for a single factor is worse than two factors, users prefer it more as the convenience factor overweights security in the user's prespective.

Table 3: Factor Analysis Table

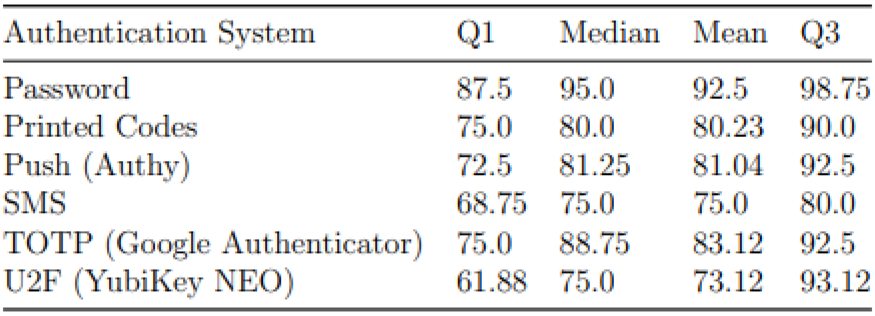


	Loadings			
	Factor 1: Ease of Use	Factor 2: Cognitive Efforts	Factor 3: Trust	Communality
Convenient	**0.91**	0.05	-0.02	0.77
Quick	**0.84**	-0.12	-0.15	0.67
Enjoy	**0.77**	0.15	0.12	0.63
Reuse	**0.75**	0.04	0.19	0.75
Helpful	**0.72**	0.02	0.17	0.69
No Enjoy	**-0.52**	0.22	-0.16	0.55
User Friendly	**0.42**	-0.19	0.37	0.74
Need Instructions	0.15	**0.80**	-0.12	0.60
Concentrate	0.03	**0.64**	0.14	0.38
Stressful	-0.41	**0.51**	0.01	0.59
Match	-0.30	**0.42**	-0.15	0.47
Frustrating	-0.47	**0.47**	0.00	0.63
Trust	0.08	-0.04	**0.80**	0.74
Secure	-0.02	0.03	**0.82**	0.82
Easy	0.27	-0.28	0.31	0.44
Eigenvalues	7.52	1.78	1.03	
% of Variance	32	15	14	
Total Variance		61%		

Factor Analysis Table by Cristofaro, E., Du, H., Freudiger, J., & Norcie, G, 2014

Table 3 above shows the usability analysis for two factor authentication variance statistics by Christofaro, E et al. (2014). There are 3 factors that determine the usability of two factor authentication which are the ease of use, cognitive efforts and trust. For each row in table 4, the bolded numbers correspond to a factor in the column while the unbolded numbers will be excluded since they are not correlated (Christofaro et al, 2014). In the ease of use column, most of the bolded numbers have a variance higher than 0.5 except for “No Enjoy” and “User Friendly". No Enjoy have a negative variance number and user friendly have a 0.42 for user friendliness. This means that most of the users do not see multifactor authentication as a tedious process but there are some individuals that see it as non user friendly. In the Cognitive efforts column, there are 3 data that have lower variance than 0.52 which are stressful, match and frustrating. This means that users are feeling a little frustrated when using the authentication system but occasionally they will feel stressed. Finally on the trust column, trust and secure have variance higher than 0.8. This demonstrates that users place their trust upon the system to protect their data from attackers. Overall, this table shows that Multifactor authentication systems are highly usable (Christofaro et al, 2014).

Table 4: Survey Scores for two factor authentication system, summary statistics



Authentication System	Q1	Median	Mean	Q3
Password	87.5	95.0	92.5	98.75
Printed Codes	75.0	80.0	80.23	90.0
Push (Authy)	72.5	81.25	81.04	92.5
SMS	68.75	75.0	75.0	80.0
TOTP (Google Authenticator)	75.0	88.75	83.12	92.5
U2F (YubiKey NEO)	61.88	75.0	73.12	93.12

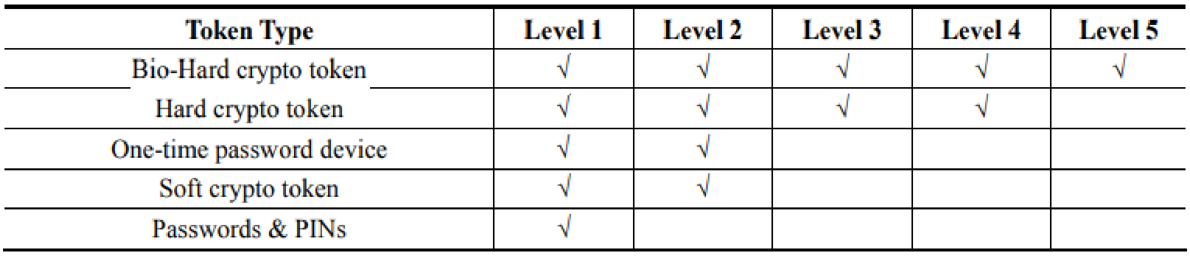
Survey Scores for two factor authentication system, summary statistics by Reese, K. R., Seamons, K., Zappala, D., & Ventura, D. 2018

The table above shows the usability rating of all the different two factor authentication systems. According to the table, the highest mean rating is password while the lowest rating is U2F authentication system. Password authentication system is the highest as it is the most popular authentication system and it is used in all of the multi-factor authentication combinations. U2F is the lowest because users would need to carry around the usb stick in order to access the system. If users have lost the usb stick, it is a hassle and difficult to create a new key.

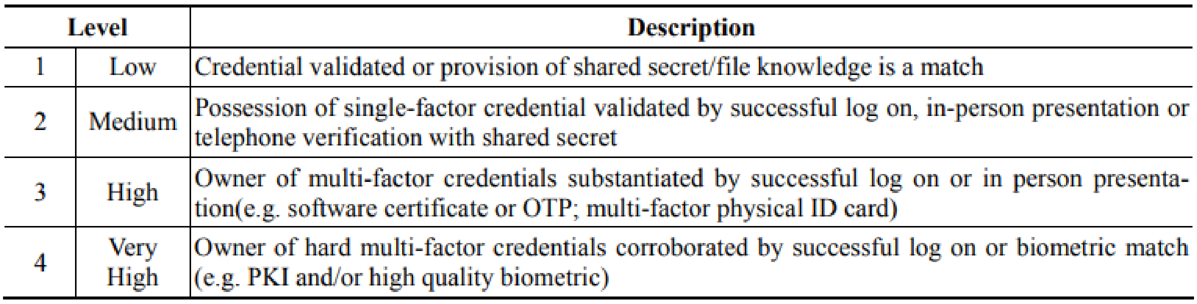
Application Protocol/System Security Vulnerability

Although multi factor authentication is a more secure method of authentication, there still exist many security vulnerabilities that could be exploited by malicious users. Firstly, as the simplest form of multi factor authentication, single factor authentication has the most security vulnerability. These are phishing attacks, malware or keyloggers, social engineering attacks, and hardware vulnerabilities.

Table 5: Token type assurance level



Token Type	Level 1	Level 2	Level 3	Level 4	Level 5
Bio-Hard crypto token	√	√	√	√	√
Hard crypto token	√	√	√	√	
One-time password device	√	√			
Soft crypto token	√	√			
Passwords & PINs	√				

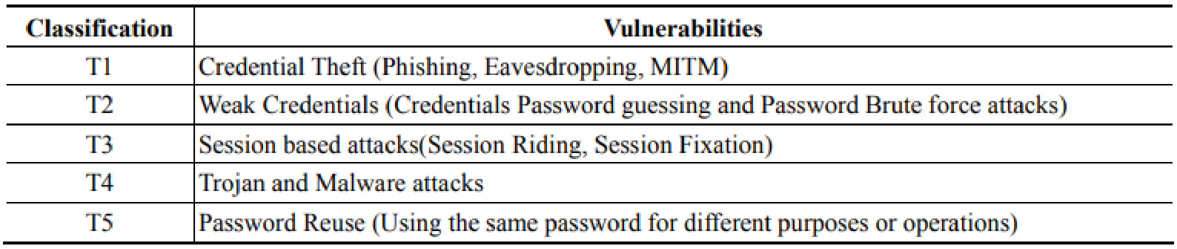


Level		Description
1	Low	Credential validated or provision of shared secret/file knowledge is a match
2	Medium	Possession of single-factor credential validated by successful log on, in-person presentation or telephone verification with shared secret
3	High	Owner of multi-factor credentials substantiated by successful log on or in person presentation(e.g. software certificate or OTP; multi-factor physical ID card)
4	Very High	Owner of hard multi-factor credentials corroborated by successful log on or biometric match (e.g. PKI and/or high quality biometric)

Token types allowed at each assurance level by Kim & Hong, 2011

The table above displays the assurance that each type of token is able to provide when using them for single factor authentication. Passwords and PINs provide the least amount of security assurance as they are high risk to malicious attacks. On the other hand, biological tokens have higher assurances as they are unique to each person and it has a higher difficulty to duplicate. One-time password devices and hardware tokens are in the middle ground as they offer a need for a secondary device to be used to authenticate the user. However, it is also possible for thefts to occur which is also a security vulnerability as well.

Table 6: OWASP Testing Item



Classification	Vulnerabilities
T1	Credential Theft (Phishing, Eavesdropping, MITM)
T2	Weak Credentials (Credentials Password guessing and Password Brute force attacks)
T3	Session based attacks(Session Riding, Session Fixation)
T4	Trojan and Malware attacks
T5	Password Reuse (Using the same password for different purposes or operations)

OWASP Testing Item by Kim & Hong, 2011

This table above describes the different tiers of vulnerability that could occur in multi-factor authentications. From the lowest tier of password reuse, where the user uses the same passwords for different purposes to credential theft through phishing or eavesdropping. These are all possible attacks for attackers to adopt for malicious intents. In general, multi-factor authentication is not invincible to security breaches, but they make such attacks exponentially harder by simply duplicating the amount of authentication required.

The countermeasures that could reduce security vulnerabilities in multi factor authentication differs from what type of authentication is required. The simplest way to prevent a brute-force attack on passwords or PINs is to implement a maximum number of incorrect attempts or CAPTCHAs at each login attempt. Cryptography and hashing are the most important countermeasures for malware lurking in the system to leak our credentials for malicious intents. At the same time, countermeasures from the user side are also very important for hardware used for one-time passwords or hardware tokens. These should be used hand in hand to protect against malicious attacks.

Critical Analysis of Results

From all the discussions above, we could observe that multi-factor authentication is an effective and secure method of authentication. However, this comes at an expense of cost and usability. While the more factors of authentication included increases the security of the system, it also drives up the cost of operations and the usability of the user as discussed above. This is because more authentication is equivalent to more time spent and more systems to support the multiple factor of authentications. Nonetheless, it is important to note that there still exist security vulnerabilities that make multi factor authentication not invincible.

It is also important for different companies in different industries to identify what is the most suitable type of multi-factor authentication for their users. For example, a bank would require at least 3 factors of authentication for most of their transactions as the security assurance is most important to their users while a social media would most likely use 2 factor authentication as the users would still want some security but with better usability. In addition, it is very crucial for them to adopt efficient and effective encryption algorithms during the transmission and storage of critical information. For very specific and necessary purposes, they could adopt Virtual Private Network to create a virtual tunnel which prevents the interception of malicious parties.

Cryptographic algorithms are crucial in multi factor authentication to ensure the confidentiality and authenticity of the user. This is because the information during transmission from the user to the server could be intercepted easily and a strong cryptographic algorithm could encrypt the message which leads to less malicious attacks being successful. This cryptographic algorithms are not just used for passwords and PINs, but also for one time passwords,

References

Abiew, N. A., Jnr., M. D., & Banning, S. O. (2020). Design and implementation of cost effective multi-factor authentication framework for ATM Systems. Asian Journal of Research in Computer Science, 7–20. https://doi.org/10.9734/ajrcos/2020/v5i330135

Ascar, A., Liu, W. Y., Bayeh, R., Akkaya, K., & Ulugac, A. S. (2020). A Privacy-preserving Multi-factor Authentication System. Retrieved March 30, 2023, from https://onlinelibrary.wiley.com/doi/am-pdf/10.1002/spy2.88

Adeyemo, Z. K., Lasisi, T. A., Akanbi, I., & Olatide, A. (2015). Data Transmission Using Multi-Factor Authentication over Wireless Communication Channel, 5(2), 73–80. https://doi.org/10.5923/j.ajis.20150502.04

Ali, G., Ally Dida, M., & Elikana Sam, A. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. Future Internet, 12(10), 160. https://doi.org/10.3390/fi12100160

Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2014). A comparative usability study of two-factor authentication. Proceedings 2014 Workshop on Usable Security. https://doi.org/10.14722/usec.2014.23025

Folger, J. (2022). What is spoofing? how scam works and how to protect yourself. Investopedia. Retrieved March 30, 2023, from https://www.investopedia.com/terms/s/spoofing.asp#toc-what-is-spoofing

Garska, K. (2018). Two-factor authentication (2FA) explained: Fido U2F. Identity Automation Blog. Retrieved March 31, 2023, from https://blog.identityautomation.com/two-factor-authentication-2fa-explained-fido-u2f

Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in Automated Telephone Banking. Computers & Security, 30(4), 208–220. https://doi.org/10.1016/j.cose.2010.12.001

Khaskheli, G. M., Sherbaz, M., & Shaikh, U. R. (2022). Users opinion regarding comparison between single-factor and two factor authentication using parameters of security and usability in social media application, 1(1), 17–27. https://doi.org/ISSN: 2710-5997

Kim, J.-J., & Hong, S.-P. (2011). A method of risk assessment for multi-factor authentication. Journal of Information Processing Systems, 7(1), 187–198. https://doi.org/10.3745/jips.2011.7.1.187

Reese, K. R., Seamons, K., Zappala, D., & Ventura, D. (2018). Evaluating the Usability of Two-Factor Authentication. Retrieved March 30, 2023, from https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=7869&context=etd

Reno, J. (2013). Multifactor Authentication: Its time has come. Technology Innovation Management Review, 3(8), 51–58. https://doi.org/10.22215/timreview/716

Richardet, R. (2023, March 17). 5 facts about the internet. SysGen. Retrieved March 25, 2023, from https://sysgen.ca/five-facts-internet/

Williamson, J., & Curran, K. (2021). Best practice in multi-factor authentication. Semiconductor Science and Information Devices, 3(1). https://doi.org/10.30564/ssid.v3i1.3152

Yasar, K., & Cobb, M. (2022, April 28). What is a man-in-the-Middle Attack (MITM)? - definition from Iotagenda. IoT Agenda. Retrieved March 30, 2023, from https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM