Master of Science in Internetworking

Mint 709

CAPSTONE PROJECT

Comparative analysis of top 5, 2-factor authentication solutions

By

Manpreet Singh Saini

Project Supervisor

Leonard Rogers

Contents

List of Figures

Abstract

The risk of online personal information breaches is increasing as people put more critical data online., strong authentication protecting this information is not being adopted quickly enough to deal with the threat. Online security specialists recommend people should use two-factor authentication (2FA) on password-protected systems to help to eliminate the account breach.

Two-factor authentication (2FA) aims to enhance the resilience of password-based authentication, typically requiring an individual to authenticate using something they know as well as something they have for example a code generated by software token or with use of hardware token along with password. Also, the typical user can only remember a small number of short passwords or they choose common passwords which eventually increases the risk of account breaches. That is why an increasing number of applications are requiring two-factor authentication.

There are many two-factor authentication products available online based of different types of two-factor authentication, for example, Google authenticator is based on software token, Yubico U2F key is based on a hardware token, Gmail offering prompt-based, security key or SMS based method for two-factor authentication and many other which will be discussed in this paper. Some of them are free and some are associated with cost.

The focus of this paper is to study and analyze various two-factor authentication based on their strength, the cost associated, use cases and other factors depending on the user requirement.

1. Introduction

Online security is crucial. The widespread use of the internet for various purposes has yielded the importance of security for devices. Particularly in Banks, Government workplaces, healthcare sector, defense association, eCommerce websites the validation of clients is currently an essential issue. Government associations are setting measures, passing laws, and constraining different organizations to comply with these measures without any resistance. Both corporate and individual resources are in danger against hackers trying to steal crucial data which could jeopardize any organization. For providing better security into somebody's account, one of the best methods proposed for end-users is creating "Username/Password" which means authenticating users on the web.

Every organization today implements the identification and authentication method for ownership rights via the 'Username/Password' method. This has become routine for day-to-day users as it is not so arduous to implement, inexpensive and ecumenically accepted all over the cyber world. Albeit, it may seem like a facile cybersecurity technique, but it is far more involute than you can even celebrate. Password management was never a simplistic task and is quite expensive depending on the requirements of the organizations. Even an amateur can download password cracking tools online and attack any user or steal confidential data. Therefore, there was a need for some supplementary technique for password protection. There are many techniques to protect your password against theft and the two-factor authentication (2FA) method is one of them.

2: Problem definition

The username/password model is most common and unique approach used for authentication on the internet. Every age group user is on the internet and is registered at various websites with the same or different passwords used by them.

So, where does the problem arise? It is based on a lack of user selection for passwords. Low-entropy passwords is a nightmare in the internet world. The American business magazine, Forbes, reports the list of worst passwords used every year. There will certainly be no substitution to the Username/Password model anytime soon but there could be some amelioration to this approach. Talking about improvements, two-factor authentication (2FA) approach was developed to provide better security to weak passwords.

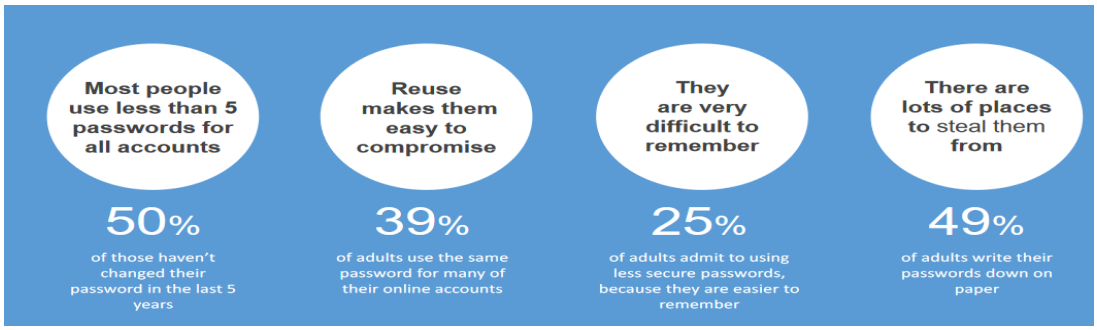

Figure 1: Trouble with Passwords [1]

This prompts the next question, which two-factor authentication solution is best for the user to increase security. Today, the two-factor authentication solutions are available in the abundance some of which are free, and some come with a cost and continuous management. In this report, I will compare different two-factor authentication solutions by reviewing the cost, strength, and the purpose behind using two-factor authentication. For instance, a user with organization critical information opts for two-factor authentication whereas it would be not a suitable approach where the user login daily to read various articles, but it should have some password length requirements

3: What is authentication?

Authentication is based on three factors,(1)the knowledge factor: something the user knows e.g. a password, PIN or a security question (2)the ownership factor: something the user has e.g. an ID card, cell phone with hardware/software token or implanted devices (3)the inherence factor: something the user is or does e.g. biometric identifier, face recognition, voice recognition, etc. [2]

Figure 2: Conceptual authentication example [3]

3.1 Detailed description of authentication types

Knowledge factors

- **Passwords**

  Most widely used authentication 'password' is a combination of words, number or special character that is required to verify the user to give access. Most user choose their password based on ease of memorization. An example of common passwords is 'qwerty','123456789', etc. and complex passwords are 'R@Awa11@@1BE', etc. Passwords are used to login to the computer, phones, IoT and some other devices. The reason behind the widespread use is the level of ease to use and cost-free. [4]

- **Credit/Debit PIN**

  All the banks in the world give the PIN to their customers for authentication. This authentication plays an essential role in the banking sector. PIN refers to a Personal identification number, is a 4-digit combination and quite easy to remember. This goes together with the password authentication type. The best thing about PIN is that if anyone does three wrong attempts then the card will be seized automatically by the bank and the owner must visit the designated bank to retrieve access to the card. [4]

Possession Factors

- **Credit/debit card**

  These cards are used to withdraw money from ATM's, for shopping. Some credit and debit cards require the user to enter the PIN and some do not. The tap system to pay any bill at any place is very commonly used in Canada. Entering the correct PIN will authorize the payment otherwise multiple wrong attempts will block the card services temporarily. [4]

- **Magnetic card**

  Magnetic cards can store some data in its magnetic strip which is made of tiny iron-based magnetic particles. These are also known as swipe cards. They are used for identification of the authorized person, grant office-level access where some staff may not be allowed, tokens, Student ID cards, loyalty cards, library card or driving license, etc. [4]

- **Smart card**

  The smart card is a physical card with a small embedded integrated chip. Like magnetic cards and debit/credit card, they are used for authentication for bank cards, healthcare, mobile communication, computer, and network security. These are portable, easy to use and lightweight. This may require the owner of the card to place in the cardholder and then enter the PIN to get authorized. [4]

- **Fobs**

  These are types of hardware tokens. Fobs are referred to as small hardware devices embedded with a program to give access to buildings, vehicles, etc. It is a new kind of key for granting access to physical objects with just a tap. These key use Radio Frequency Identification (RFID) system i.e. electromagnetic fields for identification of the tags with stored information. [4]

Inherence Factors

- **Fingerprint**

  In this, the specific user is first authorized in a database by putting his finger on the access point and next time to re-verify the user must put their finger on the access point to identify themselves. Fingerprint authorization usually requires the user to input a series of three or more fingers to create redundancy in case of any damage to the fingers. This is a highly secure kind of authentication method and is costly to install. [4]

- **Retina**

  The mechanism of retina authentication goes hand on hand with the fingerprint method. Retina authentication uses the retinal pattern to verify to a user to gain access to protected places and data. The retina is a thin tissue made up of neural cells that are in the posterior portion of the eye. This complex structure of the capillaries that supply the retina with blood and therefore, each person's retina is unique. The network of blood vessels in the retina is not entirely genetically determined and thus even identical twins do not share a similar pattern. This is also a secure type of authentication but costly to install. [5]

- **Face**

  This is also known as facial recognition which we see commonly in the phone devices today for example in Apple, Samsung, OnePlus mobile phones and in some other vendor mobile phones as well. This kind of authentication measures the spatial geometry to distinguish the feature of a person's face. This mechanism typically requires capturing the user face three to four times and then the software locates the face in the image called face detection. [4]

The above discussed are some common types of different factors of authentication. There are some other types as well such as information about the user, location factor, voice recognition, etc. [4]

3.2 Authentication schemes

There are four different types of authentication schemes:

- **Local authentication** - In this authentication scheme, each application retains data related to user credentials and typically is not shared with other applications. This scheme can result in the user of the service having to maintain and remember many different types of credentials according to the service that they require access to. As an example, it can be mentioned that different government agencies, in which each one of them offer their services, manage isolated credential databases. [6]
- **Centralized authentication** - Under this scheme, each user runs the same credentials to access the various services required. Still, each application is different and must have the interfaces and necessary agreements to interact with the central system to finally authenticate the user. In this way, the user can have easier access to valuable information across a range of services, including access to private keys that could be used to sign documents. [6]
- **Global centralized authentication** - With this scheme, the user can access the authentication services directly through a third party, so it can access all the services that they need. [6]
- **Global Centralized Authentication and Web Application** - This form of authentication, ideally for E-Government, uses common applications and web portals to access a wide range of services, from which it can use a single authentication mechanism with at least two factors, so the required services can be accessed, including the possibility to sign documents. [6]

3.3 Need for authentication

The recent studies show that almost 4.54 billion people were active internet users as of January 2020 and will be increasing rapidly in the upcoming years. [7] There is a need for security methods on the internet but there is no ideal solution to provide flawless security. Studies show that around 23.6 million people used ‘123456’ as their password everywhere, 7.7 million users used ‘123456789’, 3 million used ‘qwerty’ and ‘password’ as their passwords and many other common passwords [8], names of football teams, common names with 2-3 numerical digit at the end which were easy to guess for hackers to access user privileges.

It is alarming that there is a hacker attack every 39 seconds on the internet [9], 4.1 billion records were compromised and 2.5 billions of the breaches including username and password being hacked, cybercriminals earned 600 billion in 2018 which included selling drugs online, selling user accounts, identity theft, stealing big companies financial information. [10] There are many different attacks to crack passwords including dictionary, brute force, and rainbow table attack and open source tools like Brutus, Ophcrack, Cain and Abel, Rainbow, Key logger crack to hack passwords. The issue with passwords is that even a lengthy password including special characters, upper and lower case, digits, and special character is not enough, they may still be vulnerable to password cracking hacks.

3.4 Passwords alone are not enough

Why Single-factor authentication is no longer adequate? The above stats show that there is a need for additional steps required to secure and safe-guard user accounts and there are several different supplements on the market. In a conventional computer system setting different authentication methods have been proposed for validating users and providing access to secure data. However, the most common approach to validate the user is "knowledge-based" i.e. Username/Password combination which is a single factor authentication (SFA) method. Other methods may include you to enter four to six digits to unlock your mobile phone, face recognition, fingerprint sensor or eye scan for authorization to access secure data.

Single-factor authentication (SFA) is the most simple, user-friendly mode of authentication and widely used, although this is the weakest means of validating users. One could compromise their account by sharing with someone. However, there are many risks associated with single-factor authentication, for instance, a user forgot their password, user shared their password with someone, user-written their password on a paper and password hacking attacks, means single-factor authentication is vulnerable method to secure accounts.

Single-factor authentication (SFA) was not a reliable way to provide security which led to the development of a better solution proposed as Two-Factor Authentication (2FA) which requires two factors from users for validating users and has been widely adopted on the internet. The classic example where two-factor authentications are used are banks, ATMs, e-commerce, government, corporate sectors, and many more uses two-factor authentication (2FA) which adds a step to access secure data.

3.5 Gaps in authentication factors

- **Knowledge factor**

  This is the most used factor of authentication which includes passwords, PINs, and safe combinations. The risk associated with the knowledge factor is that the attacker can guess the password. Weak password length, common passwords, bad password management practices could be stolen easily and even sometimes a strong password has some probability of getting cracked by the hacker. Attacker can use various tools and modify them with given options in the tools to crack a password.

  This is a major gap in knowledge factor, and one should take into consideration the steps the improve the security of their password for example including special character in their password, long password length and changing passwords after some time to increase the security. For PIN or safe combination, a user should never use common dates like birth dates, months, or years. Strong passwords, random PIN are good practices to secure your account. [11]

- **Possession Factor**

  Everyone today has a possession factor that they carry and use in day-to-day life, for example, smart cards, magnetic cards, credit/debit cards, etc. These various possession factors could be valuable to some users and losing these items can affect their daily life. For example, losing a memory card with confidential information can be disastrous, losing credit card effect you financially. You should carefully while using these possession factors and always try to put them back as soon as they are done using them. You should keep a regular check on these factors and in case of missing credit/debit cards, reporting to the concerned bank authority is necessary to disable the services temporarily. [11]

- **Inherence factor**

  Biometrics systems have two common failures i.e. false-negative (FN) and false-positive (FP). When the authenticator system falsely identifies an imposter as the real owner of the account is referred to false-positive and when the authenticator system rejects the valid biometric sample is referred to false-negative. For example, fingerprint authentication is considered a safe way to provide security, but the risk associated can be a dummy finger or a dead finger getting authenticated by the system. Another limitation, a damaged finger will not be accepted by the system. One should store multiple samples of different fingers in the database to overcome the finger damage issue.

  Another factor, Retinal scan is considered a highly secure authentication method, but it is very costly to install, it will not recognize people who use contact lenses or who have any eye injury. Sound and facial recognition could also be troublesome, a user having cold can lead to the system not recognizing the voice for authentication or someone can record the account owner voice and use it to log in into their account and for facial recognition, the clarity and angel of image should be taken care while standing in front of the camera [11].

4: Evolution of authentication

- **1960s, birth of password**

  Back in the 60s, computers were slow, expensive, and huge. There were only a few organizations where computers were used back then, typical mainframe computers and they were proving to be a great asset for various tasks. To access this mainframe computer there was a need to develop such a system. MIT university came up with the solution 'time-sharing operating system' such as 'Compatible time-sharing system (CTSS)' to allow their users to access files on mainframe computers. Client access the mainframe computer through terminals and often many clients would share these terminals which led to the issue of shared file.

  To solve this issue, Fernando Corbato, an MIT researcher, later professor, and one of the developers of CTSS, solved the problem in 1961 by using passwords to protect user files on this multi-user time-sharing system. The proposed system used to validate users via password. Later, a Ph.D. researcher, Allan Scherr found some weaknesses in the password system. There was a need of improving the password system which became the main concern of cybersecurity. [12]

- **1970s, password protection using salted hash**

  After the weakness found in the password system due to password leak, a researcher Robert Morris developed a way to secure a master password file for Unix operating system. It was a bad idea to store passwords in clear text file as it could be stolen or hacked. Morris used a cryptographic concept known as hash functions to save passwords in a manner so that computers could check them without truly putting away the genuine passwords themselves.

  With time there were further developments done to save passwords more securely and continued to evolve with additional techniques. For instance, if hackers establish tools to crack passwords, the industry created stronger hash functions by adding salts to passwords, a random unique number at end of the password, resulted in more unique and secure hashes.

  In the mid-70s, discussion about other cryptographic techniques like public key or asymmetric cryptography took place. Public key cryptography involves two keys i.e. public key, which can be shared on the internet to identify the user and a private key, which is used to sign things i.e. digital signature known by the private key owner only. Public key encryption, in which a message is encrypted with a sender's public key. It involves a digital certificate which is the user's public key signed with the user's private key. The message could only be decrypted by the receiver with a matching private key. This method increased the confidentiality of the data online. This technique can be used as a factor of authentication, to verify the identity of users.

  Asymmetric cryptography and public/private keys were found first in the mid-70s, beginning with classified Government Communications Headquarters (GCHQ). While those discoveries

weren't declassified until the 90s, researchers discovered their manners to utilize asymmetric key methods in the mid-1970s, eventually resulting in three famous researchers, Ron Rivest, Adi Shamir, and Leonard Adleman, making the famous RSA asymmetric key algorithm. Digital certificates and signature have become a significant factor - explicitly, something you have - in terms of authenticating your identity. [12]

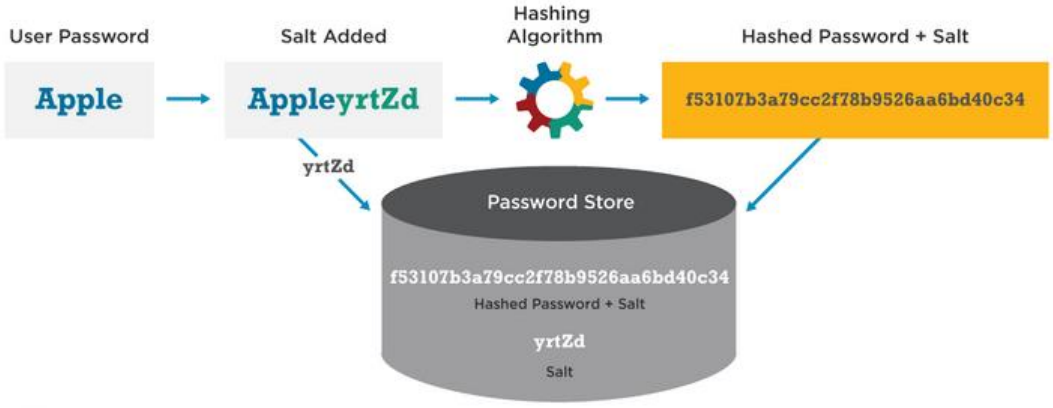

Figure 3: Salting a Password [13]

- **1980s, the emergence of One Time Password**

  As the number of active users was growing on the internet by the time, more researchers were researching new cybersecurity techniques and hackers developing tools to crack into passwords. Common attacks like brute force, pattern check, word list substitution was becoming a major concern for the internet. One of the major concerns with a normal, persistent password system is that if an attacker can guess, steal, or intercept the password then they could also replay it. To overcome this issue, One Time Password (OTP) system was developed provided uses with different password every time the user logged in.

  There were two main challenges faced at that time for implementing a one-time password system:

  1. How to algorithmically create a new, non-predictable password in a way that the server can still validate them?
  2. How to send one-time passwords (OTP) to the users.

Security Dynamics Technologies, Inc. patented a methodology in 1984 for a one-time password technique using a special hardware device and a time-based method. After a while, many OTP standards were developed with several different techniques.

There were distinct types of OTP like time-based (TOTP), oath challenge and response, HMAC-based OTP (HOTP), etc. Users would require buying a special hardware device to receive a new password every time they logon or users would get OTP through websites. From the 1980s

onwards, there was a wide range of OTP standards like S/Key and OTPW which in the long run prompted OAuth, a standard to standardize types of OTP. [12]

- **1990s, Public key infrastructure**

  During the 70s, the public key cryptography was an essential technique for authentication. Its mechanism was based on a digital certificate which proved to be a great deal for providing authentication. However, it has one issue - how might a user be sure that the public key they have for someone truly was made by that specific person? A hacker can make another public/private key pair and publish the public key as it belongs to someone else. To overcome this issue, users need some trusted third party that generates public/key pair for them, thus validating their legitimacy.

  In Public key infrastructure (PKI), a lot of technologies and standards deal with handling the public/private key or digital certificates. This infrastructure is undoubtedly bound to certificate authorities that maintain these standards, certificates, and validation of keys. As soon as public-key cryptography was introduced to internet different researcher found their ways of implementing the PKI system but officially the PKI method came into industry around the 1990s. The first official digital certificate standard, X.509 certificates, came into the business. One common example where PKI and X.509 certificates were used is Smart cards (credit cards, debit cards, etc.). These smart cards have a digital chip that held users signed public key and were managed by PKI. This technique of authentication also contributed to the emergence of multi-factor authentication.

  At this time, there were many different attacks took place. Some of them were automated and some manually done by the hacker. This is when CAPTCHAs came into play, this method does not provide authentication, but it can help the organization to get rid of automated attacks initiated by the hackers. Captcha is an acronym for “Completely Automated Public Turing test to tell Computers and Humans Apart.”

  This technique would require the users to enter a word shown on the website in distorted images which would be easy for humans to fill up but impossible for automated bots to recognize and proceed further. This helped to slow down the speed of brute force attacks, which utilizes the speed of computers to try different number of passwords until success. A straightforward method to forestall these attacks is to require a CAPTCHA arrangement with every login attempt. [12]

- **2000s, MFA became popular**

  The internet started adopting the MFA concept widely and it was evolving with time and became popularized in the 2000s. During the previous decade, there were different factors to authenticate the users online which would fall into three parts: something you know, something you have or something you are. Something you ‘know’ consists of things like a password, a

question/answer, a PIN or any mixed -alphanumeric word. Something you 'have' would be things like a smart card, a hardware device, a digital certificate, etc. Something you 'are' includes your fingerprint, retina scan, face recognition, heartbeat, voice recognition, etc.

Attackers would find a flaw in every cybersecurity technique as it came into action with time to time and there was no ideal solution to provide a flawless system. With this, researchers were also concentrating on conquering attackers' tools and techniques. They knew hackers would also leverage a way to break the new techniques of authentication. This concern resulted in wide adoption of MFA i.e. Multi-factor authentication on the internet.

Multi-factor authentication required a user to provide two or more factors to verify the identity of the person online. Two-factor authentication, three-factor authentication and as we go the authentication process becomes more complicated and is all the subset of multifactor authentication. User might require providing OTP after he enters the correct password, answers a security question, fingerprint verification, etc. The advantage of MFA is that even if the attacker is somehow able to crack the user password, it will require them to get hold onto the user's other factor too to break into their account.

MFA was there before the 2000s but was only adopted by few organizations, banks, and government sectors. For example, OTP is one of the examples of MFA which combines the normal password with a new one-time password every time. Bank or debit cards are sort of 2FA. You have a card with a chip that includes a certificate assigned to you, with a PIN that only known by the owner. Bank cards were likely to be the first one in which the 2FA method was prominently used by the users. [12]

- **2010, The smartphone era**

  Till now, passwords are the most common option for providing digital authentication. By indulging passwords with several different security practices and techniques they become a reasonable factor for authenticating users. Although the main concern with using a password is that the users do not follow the best practices, they use small, common, easy to crack passwords and even many organizations do not adopt the better methods to gain security. This sloppiness behavior leads to database leaks which demonstrate that passwords protection alone is an insufficient method to protect the user accounts.

  Since 2000, MFA helped to overcome the issue of using only one factor i.e. password for authentication however it was considered an expensive and complex method till now.

  In 2010, smartphones came with collaboration of authentication became the future of authentication. Smartphones made many authentication methods easier, cheaper, and prominent. For instance, before 2010, MFA and 2FA methods were complex, expensive, required an additional device that many users considered to be useless and unaffordable. Buying

a new device and managing it was considered an expensive and unsuitable method for many organizations.

Buying separate devices was out of budget for some companies and some of them would be just adding a number to company tax file. With the widespread use of smartphones, it and its ubiquitous nature made possible to add a factor of authentication without requiring the users to buy a new device. Everyone had a smartphone by the time and would receive OTP through texts, applications, or emails. Everyone liked this method as it was easy and did not require the users to buy any additional devices for authentication.

Another example, biometrics authentication method that scans and measure something about the user body and verify the user. It was barely used in some large companies before the smartphones came as it also required the company to install the biometric scanning infrastructure which was expensive. Smartphone companies started to add biometric scanner features in their devices to make biometric identification a reality. First came out from Apple in 2014 and FaceID in 2017.

Android devices also had the same solutions. Even getting OTP via text or application became popular, push notifications were also effective which collaboratively enhanced the authentication. Popularity and advancement in the smartphones greatly helped the community to gain access to stronger authentication methods. [12]

- **Current Day**

The last 10 years brought revolution to cybersecurity; it is easier to get hands-on authentication methods today. E-commerce websites and some other websites do online sales with the help of MFA. Data needs to be securely stored, managed online which became possible with various trends in the authentication methods. The popularity of smartphones in the last decade made authentication simpler for the users. Biometric authentication is available in almost every smartphone in today's date and everyone owns a smartphone. Every online banking organization at least uses two-factor authentication (2FA) for example combining user PIN with OTP for safe transactions online. Fingerprint authentication is used in the door entry system.

Statics shows that there were 1.8 million digital buyers in 2018 and it is going to increase rapidly in upcoming years. Hence, cybersecurity is the top priority for many businesses. There is several free multifactor authentication software available for the users like LastPass, Azure multifactor authentication, Auth0, Google Authenticator, Duo Security, RSA SecurID Access, Ping identity, Authpoint multifactor authentication and many more. All it depends on the company the choose the best practices to secure their data online and users to be more aware of techniques of combating online attackers.

MFA is the future of security and from a business perspective, the installation cost of MFA technology far outweighs the cost that would incur due to data leak or data breach. [14]

5: Single-factor authentication (SFA)

Single-factor authentication is a process of verifying users online for secure access to a given system through only one factor of authentication. Passwords have been used since the late 60s and are still used in today's world. Passwords are the most prominent example of single-factor authentication, other forms may include a PIN, an answer to a security question, fingerprint, or One-time passwords. Although Single-factor authentication is still one of the most used authentications in many areas, but it has many flaws and easy for hackers to break into users by hacking their password or other credentials. [15]

5.1 Common cyber attacks and risks to SFA

Single-factor authentication with 'username/password' has a lot of weakness which are discussed as followed:

- **Viruses and worms**

  Computer viruses are small applications that are designed to spread from host to host via a removable device. Once the virus made its way to the user network it can spread from one application to another application. Technically, viruses can be defined as a malicious program designed to spread from host to host and inject itself into legitimate applications. Once the computer gets infected with the virus it can deal a little to a lot of damage depending upon the intentions of the creator.

  Viruses spread from one device another via already infected application while worms are standalone malicious program and they rely on the computer networks to make its way through a user device. Both viruses and worms can deal with the potential amount of damage by stealing information such as passwords, bank card information and storing them online on a server designed by hackers without user awareness.

  For instance, in 1998, Robert Morris created one of the first worm named 'Morris' initially designed to find flaws in Unix system but due to some coding error, it went out on internet resulting in infecting around 6000 computers at that time and recorded as first conviction under US computer fraud and abuse act and cost around $100,000 - $10,000,000. Another example, 'Conficker' worm in 2008 infected millions of computers in 190 countries, 'ILOVEYOU' worm attacked 10 million computers in 2000 running windows operating system and cost $15 billion in recovering from the issue. Briefly, worms, and viruses related programs can steal user personal information and require some attention in combating such issues. [16]

- **Phishing**

  Old fashioned trick in which hackers disguise commonly used digital transaction websites, emails, and fool users in believing it as a genuine webpage or email. By sending fake emails, a

hacker sends a link of website which user believes to be a genuine website and directs them to input their personal information at a fake website. Phishing is a kind of social engineering technique but used on the user devices with the same objective. A hacker could send you an email posing to help you as a cybersecurity specialist and sends you a link to form where you have to input your login details, bank details or any other useful information without any risk of detection.

Using e-mails masquerading as a pay-raise notification, a modern phishing fraud duped the company employees into providing login information on a fraudulent website. Hackers gain access to within the company resources that they use to circulate a variety of malicious tools in other employee computer systems to gather more sophisticated information.

Opportunity	
Scenario Name	**Rate**
New Rewards Program	23.6%
Employee Satisfaction Survey	17.2%
Employee Raffle	15.5%
Email Migration (Data Entry)	11.8%
Corporate Rewards	9.2%
Google Docs	7.8%
Summer Flex Hours	7.3%
Email Migration (Click Only)	6.7%
Tax Refund	6.5%
Thanksgiving Deals and Coupons	6.5%

Figure 4: Phishing scenario names [17]

Social engineering is a technique where the hacker could intimate with a user, an employee of a large organization by visiting their favorite spots and indulging with them by talking about some mutual things or conflicts and could retrieve information which they would consider to be common information such as which software company user, network details, etc.

Canadian government cyber safe websites depict that about 156 million phishing emails are sent out every day, 16 million make it through filters, 8 million are opened and 80 thousand users becomes the victim and share their personal information to hackers. [18]

- **Brute force attack and Dictionary attack**

Brute force attack is one of the easiest attacks which can be performed by any amateur. Tools related to this attack is openly available on the internet which attracts inexperienced hacker to try it. In this attack, a hacker performs an iterative of submitting a user password until success. There are automated bots on the internet which can perform this attack in parallel to increase the performance of the attack. Various precaution against this kind of attack is to use a long password, brute force can easily crack any short password in a matter of time, but it would take years to crack a long mixed-alpha-numeric password with special characters. Recently, studies

show that there is a rapid increase in the number of attacks done via brute force. Therefore, every organization, user is recommended to follow the security standards to beat this attack.

Although both brute force and dictionary attack mechanism is based on cracking into user account but dictionary attack differ in a way such that it uses a precompiled list of passwords to guess such as common names, sports team names, birth dates which eventually reduces the number of combination to try to guess a password.

According to an eSentire threat report, brute force and dictionary attack increased by 400 percent in 2017 [19]

- **SQL injection (SQLi) attack**

  SQL stands for structured query language and if a form of injection attack that specifically targets SQL database server by execution of malicious SQL statement on the webpage. If successful, the hacker can steal confidential data from the database like customer credit number, social insurance number, account passwords, trade secrets, change database permissions and any other information stored in the database.

  This attack is considered as number one threat to web applications. Also, if the hacker intends to jeopardize the web application, they can do that by modifying or deleting the data from the data if they are experienced enough. However, every organization today has a backup server from where they can maintain the integrity of data if anything happens, so this attack mainly impacts the financial status and reputation of the organization.

  The success of an attack is entirely dependent on the security and configuration of the web application and database server. To conduct an attack, the attacker first inspects if the database and web application are susceptible to this type of attack. This can be determined by just entering a single quote character (‘), into the query string of a URL. If the attacker receives an ODBC error message, then the SQLi attack is possible.

  Typically, such an error message implies, that the scripts that are running on the web-based application are capable of being modified and subsequently, the attacker can inject SQL question strings and SQL server commands that do whatever the hackers intend to do.

  For its "State of the Internet" report, Akamai analyzed data gathered from users of its Web application firewall technology between November 2017 and March 2019. The exercise shows that SQL injection (SQLi) now represents nearly two-thirds (65.1%) of all Web application attacks. That's up sharply from the 44% of Web application layer attacks that SQLi represented just two years ago. [20]

  SQLi attack was discovered around the 2000s but still, it is estimated that two-thirds of web applications still suffer from SQLi attack. In 2017, more than 60 universities and government websites were attacked using SQLi.

- **Cross-site scripting (XSS)**

  This type of attack is related to the SQLi attack in which the attacker attacks the vulnerable websites to steal stored data, user credentials, etc. In XSS, the attacker targets the website user directly to steal individual information like passwords or bank information. This attack also includes the injection of malicious code into the website with the intent of attacking the user. The malicious code that has been injected only runs in the user's web application when they visit the attacked website and impacts the visitor directly, not the website. This can be done by hijacking user sessions, steaking user cookie, and phasing. For example, embedding a link to a malicious JavaScript in a comment on a blog.

  Cross-site scripting is of two types: persistent, which is possible when a web application stores user input and later serve it to other users. The attacker could benefit this by saving the malicious code in the database which later somehow went to another user browser and executed. Non-persistent, in which the malicious code is not stored anywhere instead it is executed on the victim's browser. The code is returned as part of the HTML response that is sent by the server. Thus, the user is being tricked into sending malicious code to the vulnerable website which impacts the user browser where the XSS data executes.

  In the recent research done by PreciseSecurity.com in 2019 discloses that cyber-attacks targeted nearly 75% of large organizations in Europe and North America out of which 40% cyber attacks were performed using cross-site scripting (XSS). [21]

- **Hash cracking or decrypting tools**

  As we have seen above are some common attack vectors that are used by hackers to steal organization data but stealing the data alone is not enough since long ago. Every organization use encryption techniques and hash function to store their data. The better the encryption technique implemented the harder it will be to decrypt the database files. There are some tools out there that are designed for password recovery, one example of such a tool is 'Hashcat' which offers multiple attack modes included in it. [22]

- **Social engineering**

  Social engineering is all about manipulating people into providing confidential information to the attacker which includes passwords, bank information and any information which the attacker intends to gather. Phishing technique also falls under the subset of social engineering. A hacker may get an organization's junior IT employee or administrator into revealing information like what software they are using to store data, security tools and practices implemented in the organization or even trick them into sharing half of their password details which asset the hackers to attack the organization internally.

  With the blast in the number of social sites, it has become a lot more easier, a hacker can create a fake online profile and with a fake photo of anybody and contact the employee or

administrator on some tech websites like LinkedIn, GitHub or any other code supporting website and start helping the employee such that gaining their trust and eventually having them to reveal critical information like security practices and tools used by the organization.

Other than this, Emails, phone calls where the attacker pretend to be a help desk assistant of some assistant or pose as the victim's boss or co-employee and ask about various critical information.

For example, Yahoo data breach in 2013 was done using the social engineering technique "spear-phishing". In an interview, "Malcom Palmore, the FBI special agent in charge of the bureau's Silicon Valley office, told that the initial breach that led to the exposure of 500 million Yahoo accounts likely started with the targeting of a 'semi-privileged' Yahoo employee and not top executives. He said social engineering or spear phishing 'was the likely avenue of infiltration' used to gain the credentials of an 'unsuspecting employee' at Yahoo." [23]

Other ways: Physical: passwords written on sticky notes or observed by the victim types it into their machine. If somehow anyone gets hold of the physical note of the password, then it will result in an account breach. [24]

Retrieval: An attacker answering security questions can often retrieve a password when it's stored in plain text or a reversible format. [24]

6: Industry blow-ups

Below are some case scenarios where we will see find out the vulnerabilities of single-factor authentication and where the implementation of two-factor authentication would have made a difference.

- **Operation Aurora** - In 2009 Google, Adobe and dozens of large firms were affected by the attack coming from China. The name comes from references in the malware to the name of a file folder named "Aurora" that was on the computer of one of the attackers. McAfee researchers say when the hacker compiled the source code for the malware into an executable file, the compiler injected the name of the directory on the attacker's machine where he worked on the source code [25] . It was found in a part of its investigation that at least 20 other large companies, in the areas of technology, media, and chemical, banks had been similarly targeted. Google announced this as a ‘highly sophisticated and target attack’ and the main goal of hackers was to steal the intellectual property of various organizations.

  In 2010, Google confirmed these attacks began mid-2009. The objective of hackers to attack on Google was to access the Gmail account of Chinese human rights activists. Only two of the Gmail account was compromised but the content of e-mail was not exposed, said by Google. Meanwhile, Google also found that dozens of Gmail account of active human right activists from USA, China, and Europe appeared to have been routinely accessed by third parties and believed these to be the result of a phishing scam, malware, and tailor-made Trojan attacks.

  Since then, Google has been actively working on eliminating account takeover attacks and has implemented two-factor authentication on the global platform. Two-factor authentication has helped to save a lot of users from account breaches. Google has its own Google Authenticator application and they also confirmed that the use of a hardware token as the second factor of authentication is one of the best security practices for any organization to overcome attacks on user accounts. [25]

- **Yahoo** - In 2013, Yahoo announced that it believes that 3 billion accounts credentials were stolen. Yahoo recommended their users to change their current password, change the password on other websites if they are using the same passwords and even consideration of deleting the account if there was too much risk of losing a lot of information linked to that account. Later, in 2014 it was hit again, and 500 million accounts were compromised. Using the second factor for authentication would have saved many accounts from third-party logins. Although, Yahoo later-on included 2-step authentication in its application and any user can easily set up this service. [26]

- **Deloitte Data breach** - Deloitte represents one of the big four accountancy firms and provides auditing and tax consultancy services to some of the world's largest companies, including many

banks, pharmaceutical corporations, and government agencies. Deloitte also provides cybersecurity consultancy services and is one of the most widely respected firms and was rated as the top cybersecurity consultancy firm in the world in 2012.

The Guardian newspaper reported that Deloitte discovered the hack in March 2017, but it is believed the attackers may have accessed its systems since October or November 2016. The attackers are believed to have access to the firm's Azure cloud account for months, with the initial breach believed to have occurred in October 2016. The Azure account was used to store company emails. The hacker compromised the firm's global email server through an "administrator's account" that, in theory, gave them privileged, unrestricted "access to all areas." The account needed only a single password and did not have any two-factor authentication, sources said. [27]

- **Timehop** - It is a popular app that lets its users share your past moments/posts with friends and online colleagues. It connects and retrieves posts from known media platforms, like Facebook, Twitter, Instagram, Foursquare, Google, and Dropbox. In 2018, approximately 21 million records which included personal information of users like emails, phone numbers, etc. were compromised due to data breach. Sources said compromise of an employee's account was the main reason behind this data breach. How the hacker gained employee credentials is unknown but what is known is that the Timehop cloud environment did not require any additional factor of authentication and that the compromised employee's access was enough to create additional user accounts with administrative access.

  After the breach, Timehop reportedly said: "We immediately conducted a user audit and permissions inventory; changed all passwords and keys; added multifactor authentication to all accounts in all cloud-based services (not just in our Cloud Computing Provider); revoked inappropriate permissions; increased alarming and monitoring, and performed various other technical tasks related to authentication and access management and more pervasive encryption throughout our environment." [28]

  There are many other real-life scenarios where the use of two-factor authentication would have saved many organizations from data breach attacks.

7: What is Two-Factor Authentication?

Two-factor authentication (2FA) provides an extra layer of security to ensure that the right user is trying to gain access to their online secure account. Initially, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information which means a user will now require two factors to securely login into their account. This second factor could come from one of the following categories:

- **Something you know**: This could a personal identification number (PIN), a password, answer to "secret questions" or a specific key pattern. [29]
- **Something you have**: Typically, a user would have something in their possession, like a credit card, a smartphone, or a small hardware token or a smart card. [29]
- **Something you are**: This category is a little more advanced, and might require a user for a biometric scan, an eye scan, face recognition or voice print. [29]

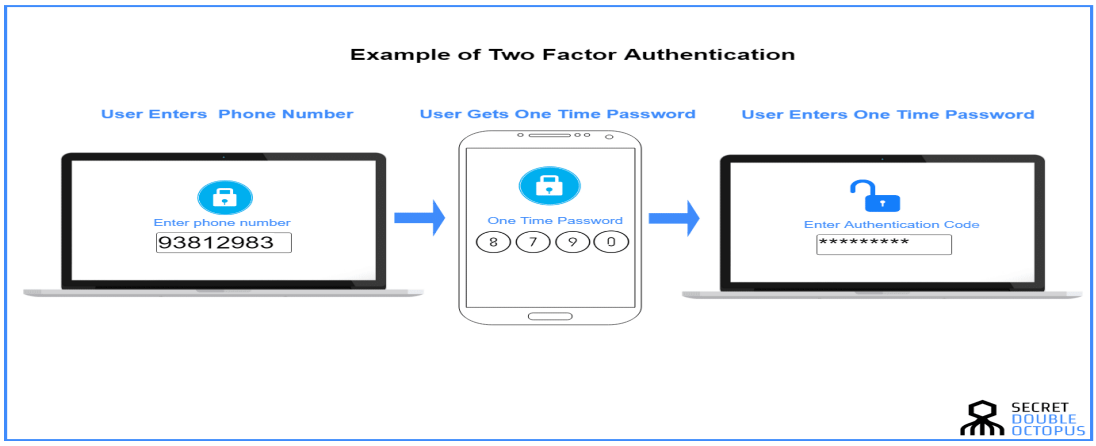

Figure 5: Two-Factor authentication example [30]

A flow diagram of OTP two-factor authentication

- The user opens the website and enter the login details and hit submit.
- The user data form is submitted and checked by the user database server on the server-side
- If the data is correct, the form requests the user to enter the second authentication factor. If the data is wrong, then the user is asked for re-entering username/password.
- On the second form, the user enters the OTP and submit it for verification
- The server-side OTP database verifies the data.
- If the OTP is correct, the user is granted access otherwise the form re-asks for OTP. [31]

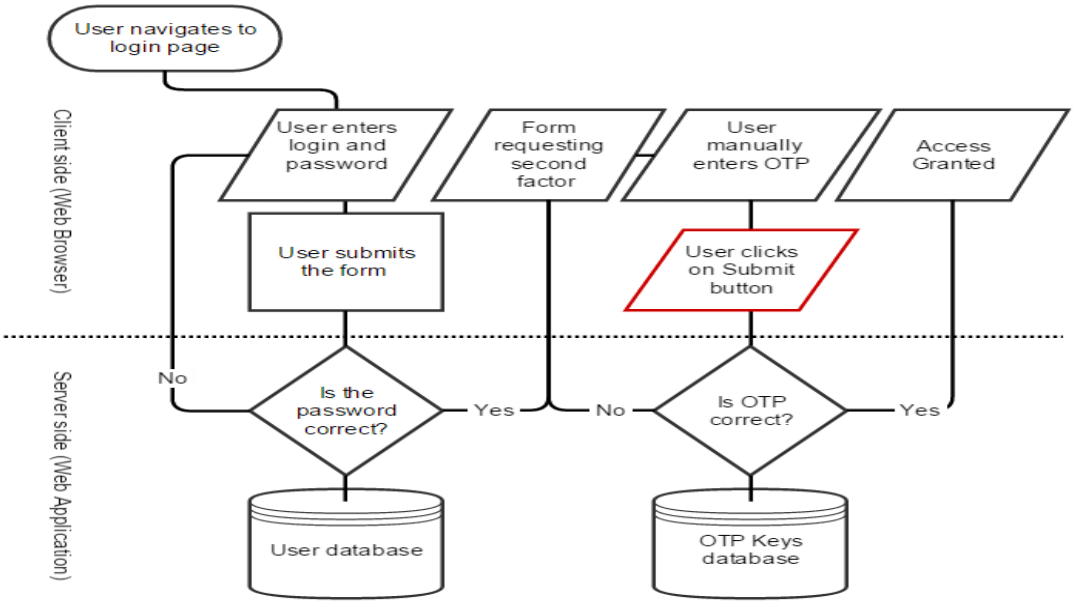

Figure 6: Authentication flow of 2FA example [31]

7.1 Detailed description: Types of 2FA

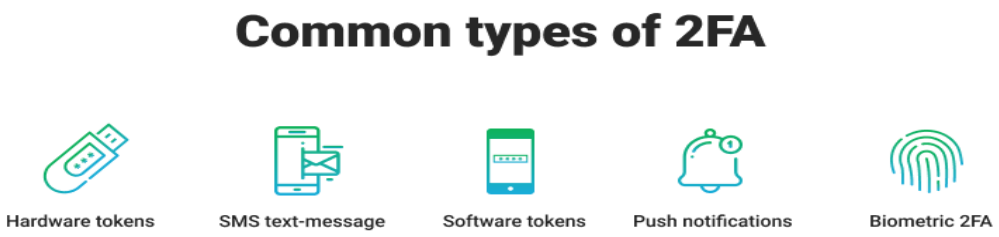

Figure 7: Types of 2FA [32]

- **SMS 2FA**

  Two-facto authentications via SMS is the most eminent method. The user will require to provide their phone number to enable SMS 2FA for a website or application they want to enable it on. After the successful implementation of SMS 2FA, the user will be asked for a one-time short code of 4-6 digits that will be sent to the user mobile phone. This method is widely used because everyone owns a mobile phone in the present time and these devices can receive SMS text.

  Although this method has some drawbacks such as delayed delivery of the message, lack of cellular service, lost network, user changed their mobile number but forgot to update the number on the 2FA website. [29]

Steps to enable SMS 2FA in Apple device

- Log in to your Apple ID account page and click on ‘Account settings.’
- Under the ‘Account setting,’ click on ‘Security section’ and click ‘Edit’
- Click on ‘Add a Trusted Phone number’ and enter the number you want to associate with two-factor authentication.
- You will get a text to verify your account first time and, in the future, you will get an SMS text code for logging into your account from any untrusted device.

- **TOTP 2FA / Software tokens**

  Time-based one-time password Is also a phone-based as well as desktop-based 2FA option which generates a unique code based on the current timestamp. This is an extension of an HMAC-based one-time password (HOTP) which generates secret keys based on hash-based message authentication codes (HMAC). It was adopted as the Internet Engineering Task Force standard RFC 6238. It is a major part of Open authentication (OAUTH) and is a widely adopted 2FA option.

  The one-time password generated must be validated in a noticeably short time as the method itself is dependent on time-based values, the validity of the code is usually for 30 seconds to authenticate the user. In case the time exceeds 30 seconds, the user will have to request a new one-time password (OTP). [33]

  TOTP 2FA overcomes the downside faced in SMS 2FA as the code generating process is not based on the server-side. Instead, the passcode is generated using the user mobile phone timestamp through an application

- **Push based 2FA**

  In this method, a user with enable push notification 2FA will receive a push notification on their device after entering login credentials correctly. This push notification notifies the user about anyone trying to login to their account and the approximate location for the login attempt. The user can approve or deny the login attempt. Push 2FA is a much more convenient option for enabling 2FA as it does not require the user to enter any code manually, the user just must tap on the mobile screen, less likelihood of user error, faster. This option eliminates the risk of the phishing attack that could be seen in SMS 2FA sometimes.

  Although, this method will require internet connectivity to send push notification to the user mobile device. The server must make sure that the push notifications are sent to the appropriate user device. [34]

  Steps to enable Push 2FA through google

  On your device, open the Gmail app Gmail. Tap Menu and then Settings and then your account and then Manage your Google Account. If you do not use Gmail, go to myaccount.google.com.

- At the top, tap Security.
- Under ‘Signing-in to Google,’ tap 2-Step Verification.
- Under ‘Google prompt,’ select Add phone.
- Follow the steps on the screen.
- When adding a phone, choose a recommended device.
- If your phone is not listed, follow the steps on the screen.
- On your device, open the Google app or the Gmail app Gmail. On the prompt, tap Yes. Your device is set up for push-based two-factor authentication
- Next time you log in from an untrusted device, you will be sent with a push notification and you can allow it for successful login or deny it in case of any fraudulent attempt.

- **U2F security keys**

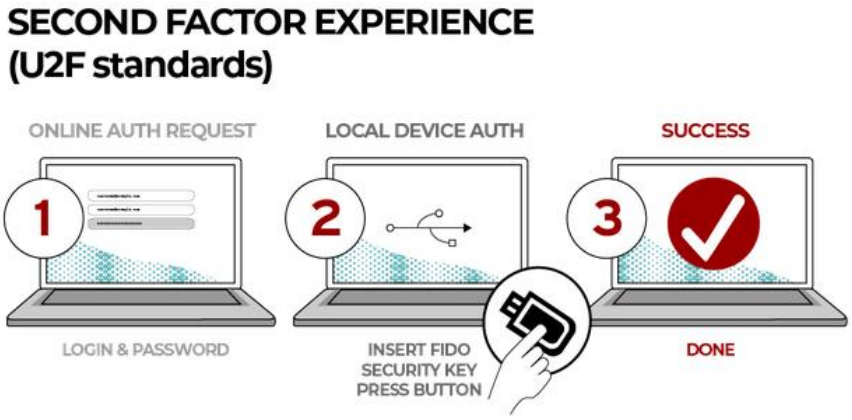

Figure 8: U2F standards example [35]

U2F referred to Universal Second Factor is a modern style of 2FA which was originally developed with the collaboration of Google and Yubico and now funded by Fast IDentity Online (FIDO). It is based on public-private key cryptography concepts. U2F secret keys could be a small USB, NFC, or Bluetooth low energy devices (BTLE). After entering the correct credential, the website will ask the user to connect the corresponding U2F key and tap it to allow login. [36]

U2F security key is an emerging option for 2FA and is supported by some browsers to date. For example, any user can simply register their device for their google account. These keys could be brought online easily.

Steps to registering U2F security key with google account:

- Open your Google account and click on ‘My Account’ ‘2-step -> verification’ and then click on ‘Learn more’ and then click ‘Security Keys’.

- Click on the ‘Next’ button and plug in the security key that the user wants to associate with their account and then click ‘Done.’
- Next time the user tries to log in from an untrusted device, the account will ask for connecting the U2F key and tap it to allow login.

Every other website that allows two-factor authentications like Facebook, Dropbox, etc. will require these simple steps to set a two-factor authentication login.

U2F key does not require the user to enter any code which makes it a very secure authentication method as it is phishing-proof. A single U2F device can be used for multiple sites to allow 2FA and it will create a different identity for each site automatically. U2F also protects your privacy. Because all the server knows is a random number and a checksum, there is nothing which identifies the key distinctively.

The drawback of U2F devices is that they are not supported by all the browsers to date. Google Chrome, Mozilla Firefox, and Opera are the only browsers that support U2F. It works on Windows, Mac, Linux, and Chromebooks. The physical U2F token works with Chrome, Firefox, or Opera, you can use it to secure your Google, Facebook, Dropbox, and GitHub accounts. Other big services do not yet support U2F. [37]

They have less mobile support as they are mostly USB devices, so the allowance of U2F 2FA is dependent on the user needs. Yubico has developed U2F keys for mobile devices as type-c USB devices but the word has not reached to many users. The users deem U2F 2FA as a costly method. Another drawback is the risk of losing the U2F devices will require the user to either disable the two-step verification from their account and remove the associated key as well or re-gain the access to account by provided methods to recover the account by the websites.

- **Biometrics 2FA: Face, Voice, Fingerprint, Retinal**

Biometric 2FA is a perfect example of using inherence factors rather than possession factors for implementing two-factor authentication on your account for secure login. The inherence factors like voice, face, and fingerprint, retina recognition can be used together with knowledge factors like username/password to implement two-factor authentication.

Like all other types of two-factor authentication types, this method also requires the same steps for enabling two-factor authentication on your account. For example, for enabling voice recognition two-factor authentication, the associated website will ask from the user to enter series of voice input for enrollment and after that, the user will have to input their voice in the system if they try to login from any untrusted device.

Similarly, one can choose for setting face, retina, or fingerprint recognition with the same series of steps. Although this method is very costly if we opt for fingerprint, retina face recognition method, their hardware installation separately requires remarkably high cost and the software

to manage such recognition must be efficiently coded. Some application supports voice recognition two-factor recognition because every device can capture audio from users. [38]

7.2 Advantages of Two-factor authentication

Below are some advantages according to business perspectives:

- **Strengthens security** - Two-factor authentication helps to enhance the account security by requiring the second form of identification. Two-factor authentication has been successful in providing better security where the users have used low-entropy passwords and helped the organizations to tackle account breaches and fraudulent transactions. For example, users can secure their Email accounts using SMS 2FA solutions.

- **Zero-Trust policy** - 2FA plays a vital role in the process of zero trust police models. A zero-trust policy assumes that every login attempt is not attempted. The added 2FA increases the probability that the user attempting to log in is a genuine user. [39]

- **Different 2FA options** - There are plenty of 2FA solutions available to choose from and the organization can implement any one of them by accessing their user needs and requirements. Organizations can choose 2FA which suites their user base, easy to use and cost-efficient. For example, a high-level security organization can opt for hardware token 2FA or biometrics 2FA solutions, mobile applications can implement SMS 2FA. [40]

- **Increases productivity and flexibility** - Every organization is providing support for mobility because it helps in higher productivity. With the help of mobile 2FA, company employees can securely access the applications, data, documents, and the organization systems virtually on any device or from any location, without putting the company network and sensitive information at risk. [40]

- **Fulfilling security compliance/standards -** Different areas like Health insurance Portability and Accountability Act (HIPPA), National Institute of Standards and Technology (NIST) recommends the organization to improve their authentication methods The NIST SP 800-63 standards are the technical requirements for authentication systems used for electronic commerce and government operations in the United States. [41] 2FA solutions are the perfect fit to meet the authentication compliances. For example, U.S. - Amendments to the Safeguards and Privacy Rules under the Gramm-Leach-Bliley Act, related to financial services, made it mandatory for banks to use multifactor solutions to prevent unauthorized user access and transactions. These proposed changes are modeled after New York's Department of Financial Services Cybersecurity Regulations that went into full effect in 2019. [42]

- **Lower helpdesk cost** - A survey by technical support industry association HDI found that around 25 to 35 percent of help desk tickets generated were due to password resets Furthermore, each of those tickets consumes, on average, 20 minutes of the help desk technician's time. Two-

Factor Authentication can help address these time-consuming and costly password-reset calls by providing a safe and secure way for end-users to reset their passwords. The business outcome includes cost savings from fewer calls, increased employee productivity, and satisfaction. [43]

- **Access control and monitoring** - 2FA supports both physical access control and data access control. 2FA can monitor and limit the access to multiple devices and provides network access control. Organizations can use 2FA access control systems to monitor and control various parameters related to payment. This helps the company security team to eliminate wastage and misuse of company resources. The cost can be controlled to a great extent with access control systems with 2FA. The company employees and administrator can limit what devices, locations or networks can access accounts and in case of any abnormal activity 2FA event triggers. [44]

7.3 Drawbacks of Two-factor authentication

- **Low adoption rate** - In addition to managing passwords users must manage the second factor also and some user deems the second factor as a burdensome method for authentication and may not like two-factor authentication. Extra security is always considered barriers from a user point of view. Two-factor authentication adds a step that a user must provide whenever they log in.

  According to a survey conducted by DUO Security, only 28% of Internet users have enabled 2FA for their accounts. Therefore, 72% of users put their sensitive information at a huge risk because the two-factor authentication is a more reliable authorization method compared to conventional passwords. [45]

- **Blocked access** - Losing the second factor for authentication can lead to user lockout from their account and gets worse if the user has not set any backup resources for recovering their account which eventually leads them to customer support desk for password change request.

  There is no certainty that the users are always carrying the second factor with them, for example, a user trying to access their email account from a new device but do not have their mobile device with them to get SMS 2FA code can lockout the user in such situation. Similarly, losing hardware token can result in the same situation. Therefore, it is always recommended to link a recovery account with your primary account. [46]

- **Sharing personal data** - For enabling second-factor authentication, the person must enter their email address or provide the phone number for SMS 2FA. Some users hesitate in providing their phone number and companies may use the personal data of users to spam promotional emails that nobody likes. Although their emails contain a link allowing them to unsubscribe, it still creates some inconveniences for users. We do not want to receive emails we do not expect unless they inform us about something important and useful.

- **Time-consuming** - As we discussed above that two-factor authentication adds a step for users whenever they are logging into their account or network. User consider it as an inconvenient method. The added authentication process with the password method can take up to a single minute to authorize users to log in and it can annoy some users. [46]

  Apple is facing a lawsuit from an offended user claiming that two-factor authentication (2FA) is a "waste of their time" for performing additional steps to log in, according to MacRumors. The complaint alleges that the use of 2FA requires "an additional estimated 2-5 or more minutes," and that 2FA cannot be disabled after it has been enabled for two weeks. [47]

7.4 Challenges associated with Two-factor authentication

- **Usability** - The biggest usability challenge for the organization is to determine the best 2FA solution according to company requirements and integrating it with existing methods. Companies are not open to the risk of changing existing applications to support a two-factor authentication solution. [48]
- **Lack of IT staff skills** - A company does not consider implementing two-factor authentications due to a lack of IT staff to manage 2FA services. IT staff will be required coaching for understanding the new working framework and might require appointing an expert to manage a 2FA solution. These added requirements will require the company to re-evaluate its budget. [48]
- **Server Maintenance** - The stakes are remarkably high while upgrading the servers to support new solutions. Generally, the companies hesitate to do so because if anything goes wrong, every associated user and employee may be affected. Ensuring the server downtime is minimum while installing new patches and application because the server needs to be restarted every time for new patches to be effective. [48]
- **Synchronization** - Real-time server synchronization is a challenge faced by some organizations for 2FA solutions. Real-time synchronization between the primary server and secondary server in case of primary server failure so that there is no issue faced with 2FA authentication request, for example, a user sent 2FA code request to the server and the primary server fails. In such a case, the secondary server should have the already generated 2FA code so that the users do not face any delayed response or denied request issue.
- **Load sharing** - Adding a new paradigm to user and employee services will require the organization to increase the server load capacity for fair utilization of the new 2FA. This might require the organization to buy more space which can cost a lot for some small organizations. Even if the organization has decided to increase the load sharing space, the IT staff would have to carefully implement and manage everything relating best resource utilization, good fault-tolerant approach and load migration time.

7.5 Considerations while buying 2FA

Planning to buy a 2FA solution? Below are some points to look out while purchasing a 2FA solution.

- **Effectiveness**

  The underlying security of the authentication method is a significant factor. One should always consider the overall effectiveness of the 2FA solution. The overall effectiveness of the 2FA solution can lead to various questions like:

  - How well it can protect against threats relating to account thefts?
  - How well the 2FA solution can integrate with the existing system?
  - Does the 2FA solution securely manage keys and data exchange?
  - What is it protecting?
  - Does it detect the compromised devices?

  If the second-factor authentication does not provide comprehensive protection, then it is not worth implementing in the organization. [49]

- **Reliability**

  You should always check the reliability of 2FA solution in various aspects such as:

  - What is the carrier-grade uptime?
  - What is the level of redundancy?
  - Is the uptime backed by service level agreement (SLA)?
  - Does the vendor offer 24/7 operation service and support?

  If the implemented 2FA solution services, go down often then there is no point in implementing such a solution as the second-factor outage can risk the organization account theft. [49]

- **Scalability**

  The 2FA solution offered should be easily scalable to handle any number of users. The organization should consider:

  - Can the 2FA solution handle growth easily at any time?
  - Can the administrator add any user to the service at any time?
  - Can the solution handle future volumes within the next 3-5 years?

  The subscription model of a 2FA solution should allow you to easily add users to the services at any time. [49]

- **Ease of implementation**

  The easier the implementation, fewer skills, and time it will take for the organization to roll out the new services to its users and employees. Various aspects can be considered for evaluating ease of implementation, such as:

  - Does the vendor provide the documentation and live support for installation?
  - Is it a cloud-based service or the organization require new servers?

- Does the 2FA solution require any hardware device for implementing?
- Does the 2FA service work natively with the type of access point in your organization?
- Do you have to install any APIs that allow you to integrate the service with the existing system?
- Can the users and employees sign up for themselves or the solution is needed to be deployed to each associated member?
- Does the user require any training to understand the working of service? [49]

- **User adaptability**

  The 2FA solution should not act as a barrier for the users. The solution should not affect the daily jobs, it should be convenient to use and flexible. Consider numerous factors such as:

  - Is it easier for a user to learn and adapt without any hassle?
  - Does the service support the Bring Your Device (BYOD) policy?
  - Does the 2FA solution require the users to carry an extra device?
  - Does the 2FA service work in case the user forgot the second factor to carry with them?
  - Can users choose from different authentication options according to their convenience? [49]

- **Reporting and maintenance**

  The 2FA solution should be easy to maintain and should be able to detect and report any abnormal activity. Consider numerous factors such as:

  - Does the solution offer real-time detection and response to security concerns?
  - Does the solution allow the administrator to set policy levels as per the organization requirement?
  - Does the solution produce log and audits trails to identify problem areas?
  - What will be the maintenance cost?
  - Are the current maintenance tasks with the service minimal? [49]

- **Total cost**

  This includes the ownership, implementation, and operational cost for buying 2FA solutions. Look for various aspects such as:

  - Does the solution require payment per device?
  - What is the new licensing cost and renewal cost for the 2FA service?
  - Does the installation require any additional resources, or it can be done with an in-house resource?
  - Does the solution require to purchase new servers?
  - Will, it cost extra to integrate the service with each system?
  - What will be the operational and monitoring cost or is it free?
  - Is the support included in the license agreement or it cost extra?

  These are some basic queries that any organization should investigate before buying any two-factor authentication solution. These queries may change according to the requirement of the

organization. For instance, which applications are at risk while implementing a new solution or how the second-factor authentication will connect with the organization Active Directory and many more questions depending upon the situation. [49]

7.6 Government Adoption of Two-factor authentication

- **Hong Kong**- The Hong Kong Monetary Authority(HKMA) supervisory policy manual module TM-E-1 on risk management of e-banking, provides that authorized institutions offering e-banking services should implement the two-factor authentication at least once for every customer's login session before any transaction exceeding HK$10,000 per day. [50]
- **Australia** - The government has directed the Australian Communications and Media Authority (ACMA) for developing new rules requiring the use of two-factor authentication to prevent fake mobile phone number porting. Telco's are expected to involve the use of two-factor authentication (2FA) - which includes an additional ID check to verify a user's identity when porting mobile phone numbers to another telco to fight scammers. [51]
- **India** - The Reserve Bank of India (RBI) mandated the use of multi-factor authentication for all the payment networks. It requires them to send an OTP or use a 3D PIN as the second part of the authentication process for every payment, which the client would receive via SMS. The client would receive an SMS of a generated PIN which they had to enter on the portal. On the Other Hand, following demonetization in November 2016, RBI received requests from various stakeholders to relax the two-step authentication process so that people could carry out digital transactions with more ease. In response to this, on 6 December 2016, RBI has released a notice relaxing the rules and saying that transactions below rupees 2,000 would not require an OTP. [52]
- **Danish Government** - The Danish Government is in the process of issuing free software tokens, used along with passwords to all citizens to promote the security of their online services. These are perceived as secure enough at this point for most public sector and private sector transactions. [50]
- **United States of America** - The US government made it mandatory for users to implement two-factor authentication to all the government domains including Federal agency, State/Local government, General Service Administration, county and any other website that uses .gov domain. The information is released on https://home.dotgov.gov/2step/. [53]
- **Korean Government** - The Korean Government is planning to have banks support one-time password systems for Internet banking. The project is being led by the Ministry of Information and Communication. The use of the one-time password system will not be mandatory but will allow citizens higher transaction amounts than the current one-time password system, which is based on cards that only store 30-35 passwords. It is not clear whether the cards are re-used or if the card is replaced after the passwords have been used. [50]

- **Malaysian Government** - Malaysian Government issues the citizen over 12 years of age with a MyKad or Government Multipurpose Card. This is a tamper-resistant smartcard which carries out the public key cryptographic operations, including those related to online authentication, supported by on-card digital certificates and a government Public Key Infrastructure. The MyKad is used for immigrants at Malaysian borders, as a driving license, to access government services online, for making online purchases, as an e-wallet, and as an ATM card with the participating banks. [54]
- **United Kingdom (UK) Governmen**t - The UK Government, is using website GOV.UK as a centralized platform for registration and authentication system called "The Government Gateway" to support safe authenticated e-government transactions over the Internet. Authentication of customers is based on either a password or digital signatures (software tokens with password protection), depending on the type of transaction. There are plans to have the UK e-ID card support a digital signature function in the future. [50]

8: Two-factor authentication statistics

Two-factor authentication adoption rates have been increasing year by year. With several possible attacks and vulnerabilities to user account, two-factor authentication proves to be the most common and easiest method to secure user credential.

The adoption rate of Two-factor authentication (2FA) was 44% in 2017 and went up to 77% in 2019 and will keep growing in the future.

In 2019 around 53% of users were using Two-factor authentication while the percentage of users using two-factor authentications in 2017 was only 28% which shows that 2FA is becoming a reliable source for securing user accounts. [45]

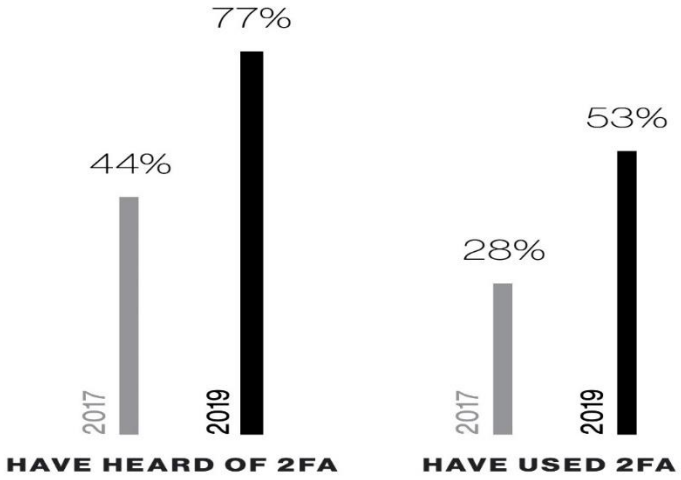

Figure 9: Adoption rate of 2FA [45]

Fig shows the importance of two-factor authentication and adoption in different areas of interest.

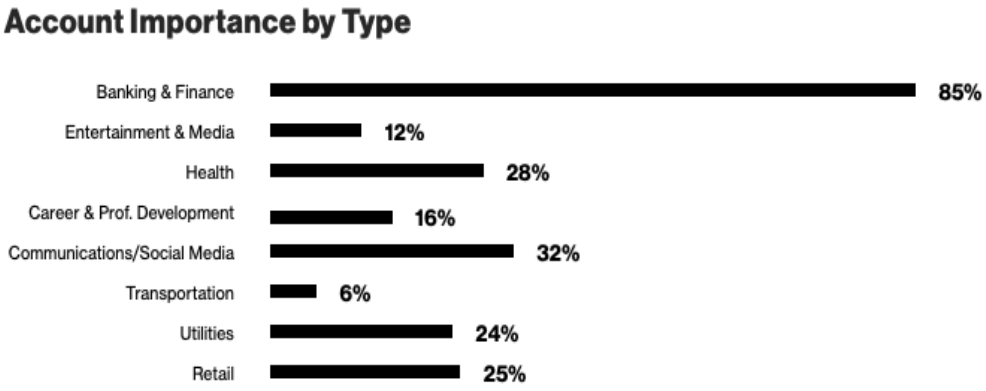

Figure 10: Account importance by percentage [45]

Fig shows diverse types of methods used for two-factor authentication and their adoption rate in 2017 and 2019.

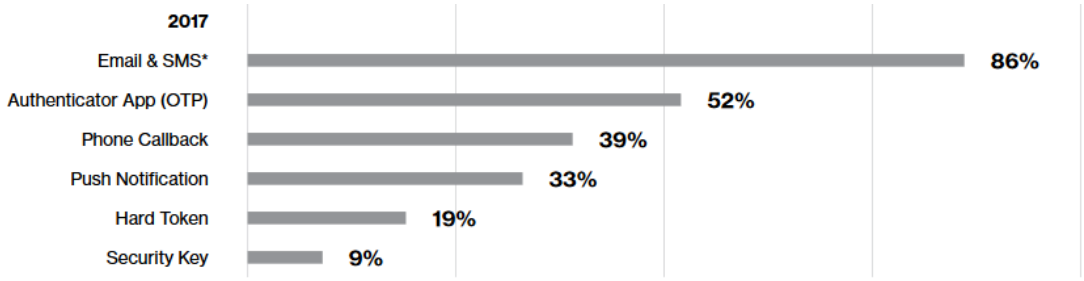

Figure 11: Types of 2FA methods used in 2017 [45]

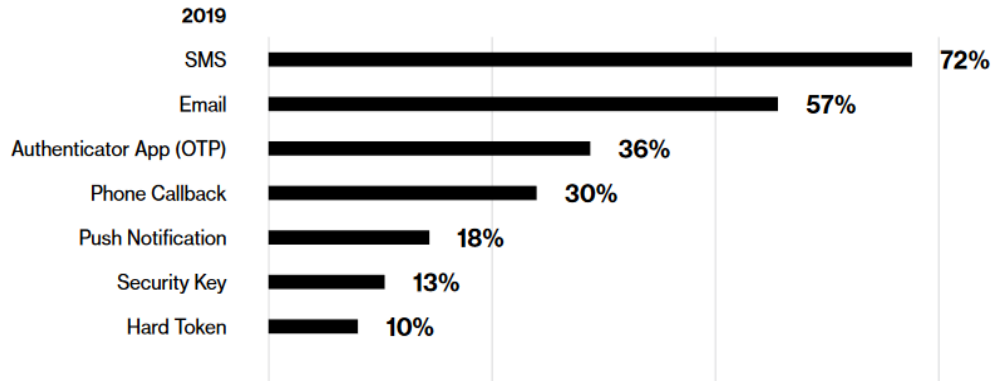

Figure 12: Types of 2FA methods used in 2019 [45]

Fig shows the reliability of one of the most common two-factor authentications: google authenticator and percentage rate of securing account against various attacks. [45]

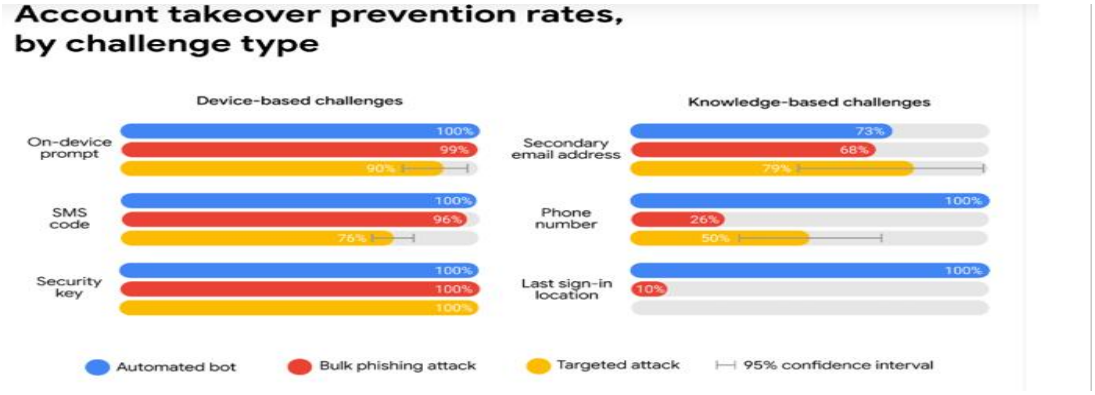

Figure 13: Account takeover prevention rate by challenge type stats [55]

9: Use cases and case study of Two-factor authentication (2FA)

9.1 Use cases

- **SMS** - The user having a registered mobile device is capable of SMS 2FA solutions. For registration, the user registering on a new website will be prompted to enter their phone number and the website will send a verification code to use mobile as a second factor of authentication. For device authentication, the user visiting the same website with a new device, the website will notice the user is using a new device to log in and will send a one-time verification code via text to authenticate the device by entering the code for validating the device for future use and same can be seen in case of a user trying to log in from new IP address.

  For money transfer validation, the user with an authorized phone number on a website will receive a one-time verification code for completing the payment transaction. Similarly, it can be used to reset passwords, for e-purchase with your credit card.

- **Legacy applications** - Adding two-factor authentications to legacy applications that do not use simple authentication protocols like SAML and RADIUS. Rather than upgrading the application with long codes, the organization can add up second-step authentication to verify its users along with a strong firewall that can enhance the security constraints and even save the modification cost of application. [56]

- **Enhancing Active Directory identity stores with 2FA -** Adding two-factor authentication can strengthen the traditional Remote Dial-in User Service (RADIUS) or Active Directory (AD) identity stores. By linking both, the Active directory can verify the identity of the user and the second factor can ensure that the user is genuine. The second factor can eliminate hackers from gaining unauthorized access. [57]

- **Web services authentication** - Two-factor authentication can be used as the identity provider for a web service like Google Docs or Salesforce cloud apps. In this scenario, a login request uses the Security Assertion Markup Language (SAML) and trusted certificates between the app and the multifactor server for the additional authentication step. This is the method used by Google and Apple to add second factor features to users' Google accounts and Apple IDs, respectively. This can also improve the security where the organization has a policy of bring-your-own-device (BYOD) as there could some malicious software residing inside the user device which can lead to compromise of user account.

  This can save the security cost for the application as the organization does not have to employ a high-end IT staff team to improve login security through coding, adding a simple step can help to improve the security. Cloud applications, organizations that offer Software as a service (SaaS), platform as a service (PaaS), like GoogleApp, Dropbox, Window Azure, OpenShift,

etc. can integrate two-factor authentication to enhance the account security of their users. SaaS is becoming a popular service and has an increase in its user base every year which also attracts the hackers to target these applications. So, adding a second step of authentication can save many users from the account breaches attack. [56]

9.2 Case studies related to two-factor authentication

- **GOV.UK** - UK government established a website, a single platform to find online government services and information. The idea was to replace multiple individual websites of different government departments and public sector, bringing everything under a single website to become efficient, single destination hub for multiple ministerial departments and organizations that provide information to millions of citizens and residents.

  It has not been an easy task to provide a single platform for a wide range of services, providing high-level efficiency and cost-effectiveness of the website to citizens and residents. The government was also interested in exploring innovative methods to bring services online on a single website.

  To implement identity assurance, 'GOV.UK VERIFY' system was developed by the UK Government Digital Services (GDS). The system was based single trusted login for the website, asking the new user various set of questions to prove their identity and verifying users in 5 to15 minutes. It allows users to choose one of several companies to verify their identity to a standard level of assurance before accessing 22 central government online services. This main objective of GOV.UK VERIFY was to securely prove the identity of a person so that they can use online government services like tax filing, driver's license information, child benefits, etc. safely and easily.

  However, weak passwords left UK government agencies and their residents exposed. The government wanted to implement a stronger authentication method to enhance the existing verification process. Low-entropy passwords usage from authorized users increased the risk of account compromised. Single level of authentication was not enough to safeguard the personal user information and online services available on GOV.UK. The government realized the need for a strong authentication scheme and considered different two-factor authentication solutions that were flexible and cost-effective to serve multiple users.

  GOV.UK was able to provide a strong authentication scheme to verify their visitors online with help of Yubico two-factor authentication solution and the GOV.UK became the first government service in the world to have a hardware-based second-factor authentication using the FIDO U2F authentication standard.

  With the collaboration of Yubikey with the existing scheme 'Digidentity,' the government was able to achieve a simple yet strong authentication solution and eliminated the risk associated with weak passwords. Digidentity is, one of UK government's certified identity providers, who

verify and confirm a user's identity before they can access a government service, The Yubikey can be easily purchased online and the user can simply register their key at the website.

Digidentity and Yubico have now put an industry-leading two-factor authentication solution in place, which is the new standard for governmental services delivery and a straightforward way for residents to access various government services online. To authenticate GOV.UK Verify using Digidentity with FIDO U2F, the user simply enters their username and password, and then inserts and taps the YubiKey.

This scheme does not require the users to install any additional software to verify themselves. Since then, the GOV.UK is delivering a high-end online service with an enhanced authentication method to its users. [58]

Understanding U2F working

U2F method challenge-response protocol based on public-key cryptography which eliminates phishing and man-in-middle attacks. It consists of two flows: registration and authentication. It also offers applications specific keys, device attestation, and device cloning detection.

The U2F device has a private key k_{priv} and the relying party has corresponding public key $k_{pub.}$ The keys are generated in a tamper-resistant execution environment.

For protection from Man-in-middle and phishing attacks, the U2F device verifies the origin of URI (Uniform resource identifier) which helps to mitigate the phishing attack and TLS channel ID to eliminate man-in-middle attack.

Application-specific keys will prevent the relying parties from tracking devices between different user accounts. This means that any website cannot know whether User1 and User2 share the same device. The U2F device creates a new key pair and key handle for each registration. The handle, h, is stored by the RP and sent back to the device upon authentication. This way, the device knows which key to authenticate with, e.g. User1's key or User2's key. The key handle is stored by the server together with kpub. The App ID, a, is being used for scoping a key handle.

Yubikey keys cannot be read externally due to its tamper-resistant environment nature. However, to provide a clone detecting service to the U2F device without tamper-resistant secure elements (e.g. software implementations), an authentication counter is used. The device increments the counter when authenticating and the relying party verifies that the counter is higher than last time. The counter is sent from the U2F device to a relying party.

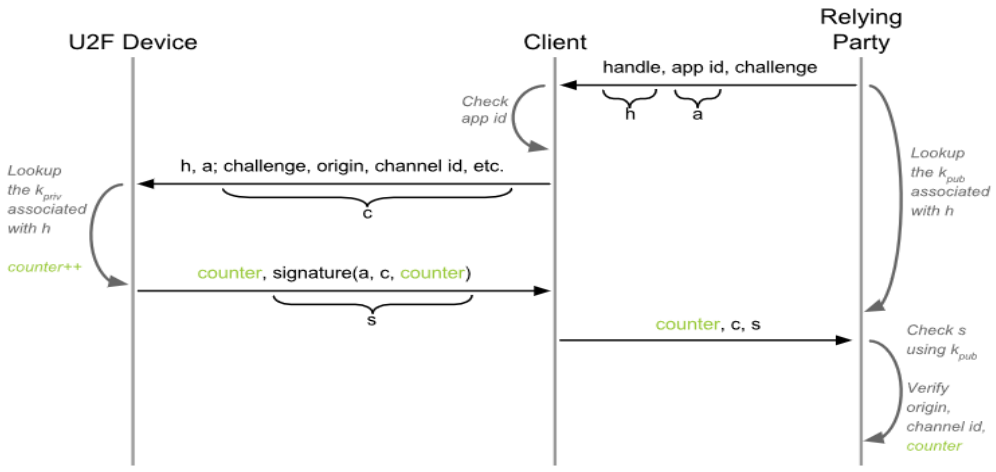

Figure 14: U2F technical diagram [59]

Verifying token properties from relying party side is done by the Attestation concept. It is implemented via an attestation certificate which is signed by the U2F device and sent to relying party upon registration. [59]

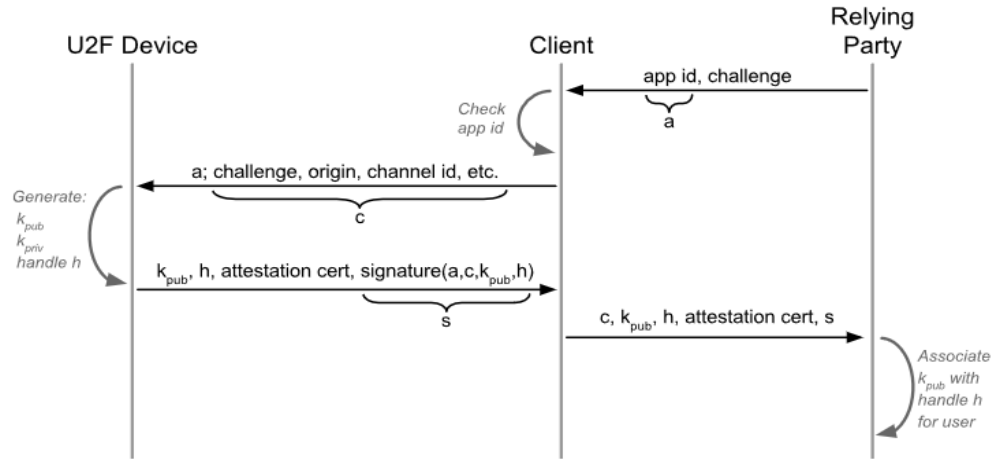

Figure 15: U2F technical diagram [59]

- **National Cyber-Forensics & Training Alliance (NCFTA)** -NCTFA, a non-profit organization that specializes in information sharing among cross-sector industries, law enforcement agencies, and academia chooses to implement a two-factor authentication solution by Duo to protect its users against online threats.

  NCFTA team lead, Julie Dunn stated, “The process of applying Duo’s 2FA service was easily applied not only for our developers but also our daily administrators that are creating new user

accounts for our partners. The ease of use, service flexibility and responsiveness of their support team made a significant difference in making our application that relies on 2FA successful."

The Challenge

In 2016, NCFTA prepared to launch a new external-facing web application that enabled its partners to share specific threat information. NCFTA is an enterprise built on trusted information sharing. Julie Dunn, NCFTA Team Lead, explains "NCFTA operates in an environment where traditional log-in information like a username and password security is not enough. That alone creates a false sense of security and can be easily compromised."

The Solution

"Adding two-factor authentication is a responsible layer of security needed for an external-facing application," says Julie. "In general, two-factor provides additional user confidence when accessing information and it goes a long way towards securing that information without much effort from our end-users and administrators. Two-factor enhances NCFTA's ability to validate and confirm who users are and when they are logging in, to help us better ensure that those users are who they say they are." [60]

- **Stinson Leonard Street -** A top national law firm needed to protect their employees from phishing and credential theft. They chose Duo for its flexibility, proactive support, and multiple two-factor authentication methods. Director of Information Security and Business Continuity, Nicholas Pelczar, stated "The Customer Success team continues to check in with us monthly. That commitment to excellence is rare and not present with every organization that we do business with. We are now asking others to be as committed to their product as Duo has been." [61]

  Stinson Leonard Street LLP is an established top national law firm that offers sophisticated regional and national practices in key areas such as banking and financial services, business and commercial litigation, employment and labor law, and intellectual property and technology. They have 14 offices in the United States and serve a wide range of clients in almost every business area.

  The company has already deployed a top security program but there is no ideal solution available for providing security. With the increase in the number of phishing attacks and credential theft, the company contacted Duo security firm for security solutions. The company faced the challenge of securing multiple remote access services used daily by its staff. They wanted to have a single security platform that could also provide multiple two-factor authentication methods, as well as one that was flexible enough to support a diverse user.

The solution

The company was a two-factor solution, the company was able to limit threats against their employees and this added an extra step for their user account protection. Nicholas and the team also appreciate the ability to monitor access from a single, centralized source.

Stinson Leonard has also been able to accumulate a new insight and drive additional security initiatives based on the information provided by Duo. During monthly talks between the Duo's Customer Success team and Stinson Leonard, Nicholas has been able to develop new insight to inform additional security strategy. [61]

Understanding Duo

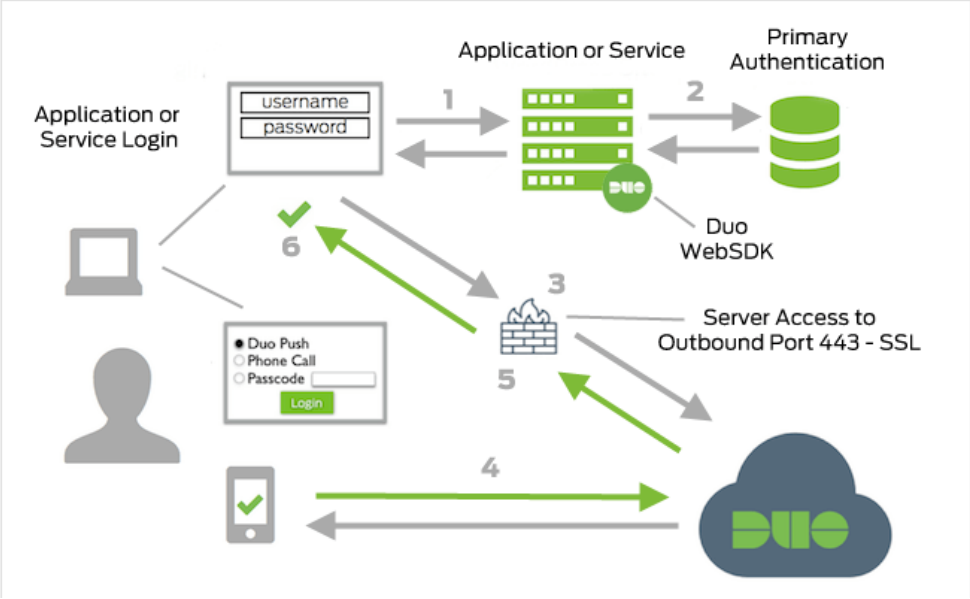

Figure 16: Duo's Network diagram [62]

Web Application or Service connection initiated in the first step. Next, the primary authentication method plays the role of verifying the user data. If the input is incorrect the user identification fails. Till this point, there is only single-factor password authentication which can be bypassed by hackers using various tools or methods.

To improve this, Duo's two-factor authentication comes into play. The web application or service connection establish connection is established to Duo Security over TCP port 443 which provides the secondary authentication via Duo security services. After this, the web application or service receives a response authentication response from the Duo server which identifies its valid users via second factor. Once the user provides both authentication factors, the web application allows the user to access the website data [62].

- **MD Live** - MDLIVE is a telemedicine provider. The company offers patients, health plans, health systems, and self-insured employers with access to board-certified doctors, pediatricians, and licensed therapists. Consultations are performed via online video, phone, or mobile app.

  The organization decided to become HITRUST Certified. Under the Health Information Trust Alliance, they were required to implement a multi-factor authentication (MFA) solution for remote access. With the users all around the globe, the company needs to increase the account security for its users.

  The challenge

  MD Live has a large user base with users from all over the world to visit medical professionals at any time of the day. This has been made possible by the company through a mobile application that allows the patients to contact the health specialist from anywhere around the world. With popularity and an increasing number of users, the risk of security threat also arises. The company's goal is to protect the patient information at any cost because the patients are trusting the application and revealing sensitive information related to their problems to their physicians through the application. MD Live stores the patient information to keep track of patients with various prescription details, their physician, appointment details and cost associated with each session.

  The company has decided to become more recognized by becoming HITRUST certified under the Health Insurance Trust Alliance as a body with strong data security as part of its health information systems. To achieve this goal, the company required to implement a Two-factor authentication solution for its mobile application.

  Vice President of Information Technology operations of MD Live, Anthony Mott, began assessing the LoginTC solution for two-factor authentication with collaboration of RSA and Yubico products. The challenge for MD Live company is in choosing the two-factor authentication solution was to choose a cost-efficient solution with ease of integrating the solution with the existing domain server without any service disruption.

  Solution

  MD Live IT team evaluated different two-factor authentication solutions based on cost, end-user acceptance and ease of implementation and opted for LoginTC two-factor authentication service. The users from different regions accessing the MD Live application services now must identify themselves using two-factor authentication to eliminate the risk of account compromise.

  One of the main reasons for researching a multi-factor authentication solution is compliance for better cybersecurity practices. Deploying LoginTC's second-factor authentication solution allows the company to comply with various requirements announced by the Health Insurance Portability and Accountability Act (HIPAA), HITRUST, Payment Card Industry (PCI), etc.

"I would recommend LoginTC for two reasons. First, your customer support is superb. Second, LoginTC has been stable. I have never had a user complain that they were not able to login due to 2FA issues. LoginTC always just works. That in and of itself is worth a lot."- Anthony Mott, VP of IT Infrastructure. [63]

Understand LoginTC working

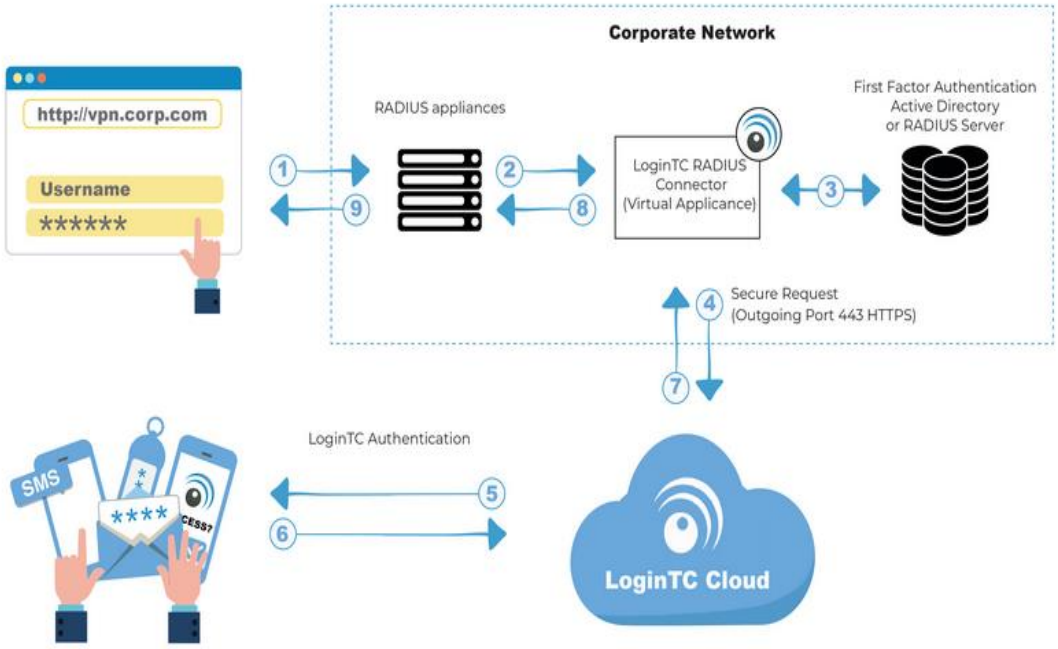

Figure 17: LoginTC 2FA architecture [64]

- A user attempts to access their existing VPN client with username/password.
- A RADIUS authentication request is sent to the LoginTC RADIUS Connector.
- The username/password is verified against an existing first-factor directory (LDAP, Active Directory or RADIUS)
- An authentication request is made to LoginTC Cloud Services
- Secure push notification request sent to the user's mobile or desktop device
- User response (approval or denial of request) sent to LoginTC Cloud Service
- The LoginTC RADIUS Connector polls until the user responds or a timeout is reached
- RADIUS Access-Accept sent back to VPN
- User is granted access to VPN [65]

10: Top 5 2FA solution

10.1 Symantec VIP intelligent authentication

Introduction

The Symantec Validation and ID Protection (VIP) Service provides a two-factor authentication solution that uses smartphones to supplement the primary username/password logins on a variety of servers and services. Symantec VIP intelligent authentication is a risk-based authentication method. The VIP Intelligent Authentication is different from the conventional enterprise two-factor authentication approaches that depend on the one-time-password tokens to strengthen password-based authentication. The VIP Intelligent Authentication examines the user's endpoint device and the user's login behavior every time to assess the likelihood that the login originates from a genuine, legitimate user.

Fundamentally, VIP Intelligent Authentication allows the user's device to act as the "something you have," and the user's behavior to provide the "something you are" factor. In any unanticipated situation which does not match the user login behavior, the VIP intelligent authentication sends secret code as a second factor to verify the users. Such an approach has the benefit that the process of authentication is invisible to a legitimate end-user, creating a simple and transparent login experience.

Transparent authentication process - When integrated with a company or web-based application, VIP Intelligent Authentication transparently assesses the risk associated with each authentication attempt by examining the user's device, its configuration, its geographic location, and its network origin. With any malicious login or unanticipated user behavior, the server sends code to the user. VIP Intelligent Authentication sends a security code to the user by SMS text message, email, or a voice phone call, and the user will need to enter that code to complete the authentication challenge. Users that are failing to complete the challenge will be denied accessing the application or network. After entering the correct code, VIP intelligent authentication validate the device and grant access to the genuine user.

The diagram illustrates the two-authentication process based on the low and high-risk login attempt respectively.

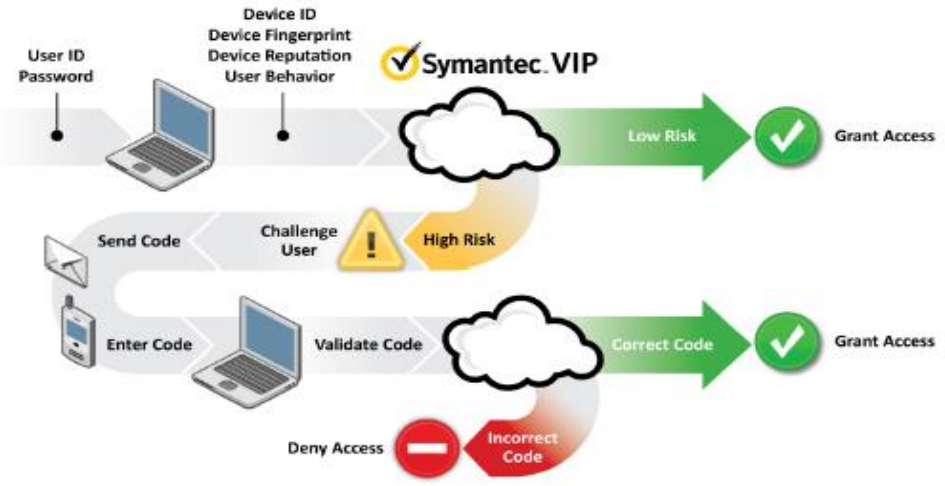

Figure 18: Symantec VIP authentication process [66]

Generic integration model for Enterprise

VIP Intelligent Authentication can be integrated with any enterprise web-based application that allows an administrator to customize the application's HTML login page to include personalized HTML and JavaScript.

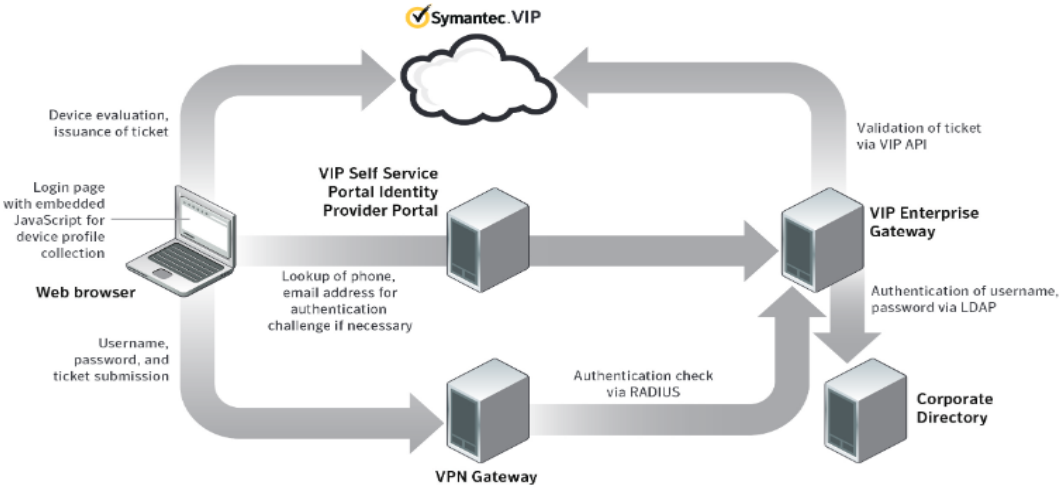

Figure 19: Enterprise integration diagram [66]

VIP JavaScript Library - To enable VIP Intelligent Authentication to gather device information, the organization will need to incorporate the VIP JavaScript library and method calls into the HTML for their application's login page. This JavaScript library and code allow VIP Intelligent Authentication to gather device information, as well as read the persistent device tag to identify the device [66]

Symantec VIP Enterprise Gateway - The VIP Enterprise Gateway acts as a bridge between the company's application and Symantec VIP cloud-based infrastructure. Once VIP intelligent authentication determines that a login attempt is from a valid user, it will generate a ticket and pass it through the login page integrated with JavaScript. The company's application will authenticate this ticket by passing it to the VIP enterprise gateway via Remote Authentication Dial-in User Service (RADIUS) protocol and will authenticate the ticket against the SymantecVIP service. For those enterprises that do not support RADIUS on-premises, SymantecVIP provides plugins for a wide variety of application plugins designed to enable such applications to connect to VIP Enterprise Gateway to access two-factor services. [66]

VIP Self Service Portal Identity Provider Proxy - The VIP Self Service Portal provides VIP Intelligent Authentication with a method to determine the phone number or email address to be used for out-of-band authentication challenges. The primary objective of this proxy is to provide the VIP JavaScript library with the capability to safely obtain this information from the organization's corporate directory directly at runtime to send the secret code to the user by using the provided information. [66]

Features:

- **Cloud-based infrastructure** - Symantec VIP offers cloud-based infrastructure, which is secure, reliable, and scalable according to the organization's future growth without needing to install any dedicated on-premises server. [67]
- **Variety of two-factor tokens** - They offer hardware tokens, free OTP software (for desktop and mobile), out of band support via SMS, voice phone calls or emails. It also offers passwordless authentication and Push-login authentication options. [67]
- **Enterprise infrastructure support -** It is easy to integrate with popular VPNs, webmail's, applications, and user AD. [67]
- **VIP application integration** - Add up strong authentication using the VIP web services API in your preferred programming language or embed VIP into your application with the VIP credential Development Kit. [67]
- **Mobile App Risk Detection** - It denies request to compromised devices before they can attempt authentication on to the network, and track threats from a single online console [67].

Benefits: Strong protection with risk-based authentication approach, increased user productivity and adoption with different token options as per the user convenience, reduced cost and complexity as it does not require to install any dedicated server on-premises, easily scalable due to cloud-based infrastructure, future proof as it is easy to send updates through cloud-based infrastructure to block and tackle new attacks and user-friendly. [67]

Maintenance and troubleshooting - Maintenance is included in VIP cloud subscription offered by them, free of cost version updates within every 6 to 12 months period, rapid response from technical support 24/7 yearly to solve issues and minimize the downtime and provide regular product updates as well. Maintenance must be renewed usually after a year. They have documented different issues support at their website - https://support.broadcom.com/. One can look up there for known issues of call the technical support. Another support can be found at Symantec.com's help page.

Security Standards - The Symantec solution supports the National Institute of Standards and Technology (NIST) levels of assurance requirements (Special Publication 800-63). [68]

Release Notes: The latest release note was published in September 2019, which means the developer is still updating and sending new patches for the product and solution.
Note - There may be latest updates released as this research was done at the end of 2019.
More information about the latest release notes can be found at Symantec.com's release note page.

Product license terms: To buy license the user can register themselves at the Symantec.com's webpage or email to the Symantec Customer Care team at customercare@symantec.com during the registration process of the asset. The buyer can either buy a permanent license or evaluation license (trial license for 30-60 days only). The payment is non-refundable.

Pricing: There is no official pricing quotation from the vendor. The organization must contact the vendor to get a quote.
Based on an article, it costs 2000 USD for setup and 5500 USD license fee yearly per 100 tokens. Article name “9-vendor authentication roundup: The good, the bad and the ugly” published at the Network world.[126]
Note: The cost estimate is based on an article and could be different at different resources.
Free Trial: Symantec VIP does not offer any free trial.

Uptime backed by Service Level Agreement (SLA) - 99.5% [69]
Note- Here uptime is calculated on a rolling 90-day basis percentage

VIP intelligent security feature - VIP intelligent authentication identity of the user device, location of the device and behavior of the user and their device against the profile collected on during each successful sign-in. Several failed logins also increment the risk score to avoid a hacker trying to enter user account using different techniques or devices.

It calculates the risk score on each login attempt based on the above assumptions and rate them between 0 to 100 to identify potential risks. It assesses the normalized risk score generated through this process versus a risk threshold specified by the administrator. Risk scores above the threshold trigger an out-of-band challenge process and require the user to enter a security code sent by VIP to the user via SMS text message, email, or phone call.

It also offers free Symantec VIP Access Desktop Symantec desktop client application that offers VIP Intelligent Authentication with access to unique, hardware-based identifiers embedded in the user's device. These identifiers help or allow the VIP Intelligent Authentication to track a user's device over multiple logins with a higher degree of confidence versus the clientless device identification option supported by VIP Intelligent Authentication. [66]

Antivirus - Symantec VIP Intelligent Authentication also offers Norton or Symantec Endpoint Protection installation to evaluate the health and trustworthiness of the user device. VIP Intelligent also can examine the number of infections reported by the machine, the number of known-bad files submitted by the machine, and the timestamp of last infection report submission by the machine. All the information collected by the Norton and Symantec Endpoint Protection installations is shared with Symantec with the consent of the user. This information can help to track devices that have an increased risk. [66]

Lost your Token?

Symantec VIP offer Lost Token Self-Serve that first authenticate the user's information like SMS, voice or Email stored in Active Directory. The VIP administrator must enable temporary security codes in the VIP Manager, enable automatic distribution in VIP Enterprise Gateway and set a temporary security code policy in VIP Manager. SMS and phone call code sent will deduct some cost [70]

10.2 Duo 2FA

Introduction

Duo 2FA offers to strengthen your applications by using a second source of validation, like a phone or token, to verify user identity before granting access. Duo is engineered to provide a simple, streamlined login experience for every user and application, and as a cloud-based solution, it integrates easily with your existing technology.

Duo has Duo Network gateway with which the corporate users can securely access the internal web applications from any device, using any browser, from anywhere in the world, without the need to install or configure remote access software on their device and they even offer self-enrollment process to make it easier to register your device or phone by yourself for second-factor authentication. Users can also connect remotely through SSH to configured hosts via Duo Network Gateway after installing Duo's connectivity tool, giving server access without a VPN.

Users first authenticate to Duo Network Gateway and approve a two-factor authentication request before they may access the different protected services. Session awareness minimizes repeated 2FA prompts as users access additional services and hosts via your gateway. Duo Network Gateway gives you granular access control per web application, set of SSH servers, and user groups. You can also define various policies to make sure only trusted users and endpoints can access your internal services.

For example, you can require that SharePoint users complete two-factor authentication at every login, but only once every seven days when accessing some other application. Duo checks the user, device, and network against an application's policy before granting access to the application.

Network Diagram

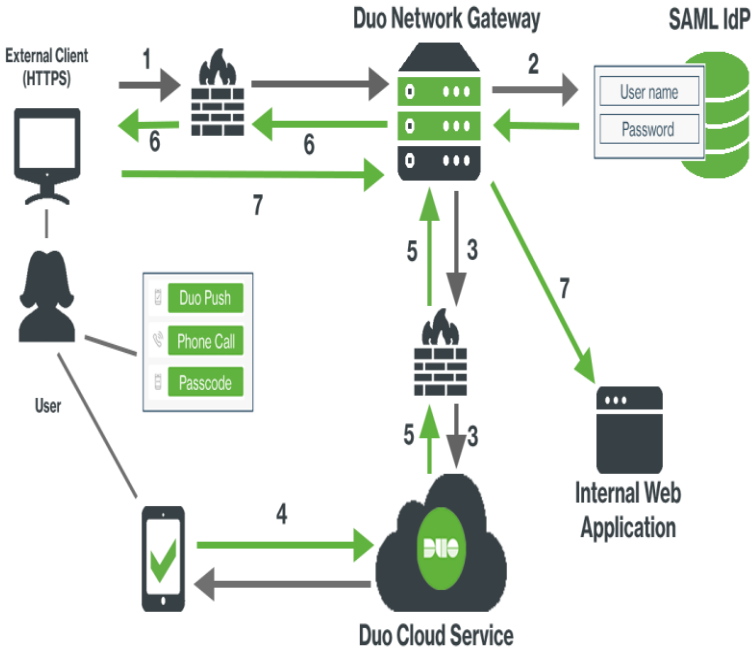

Figure 20: Web application diagram [71]

In Fig 20.,

1. The user makes an HTTPS connection to the Duo Gateway network. Next,
2. The primary authentication username/password occurs with SAML identity provider standards.
3. After entering the correct username/password, Duo's Network Gateway connection is established to Duo Security over TCP port 443.
4. Two-factor authentication occurs via Duo security service and
5. After entering the second factor the Duo Network Gateway receives authentication response.
6. With the correct second factor input the Duo Network session is authenticated.
7. External SSL will be able to access internal web application running via Duo Network Gateway reverse proxy [71]

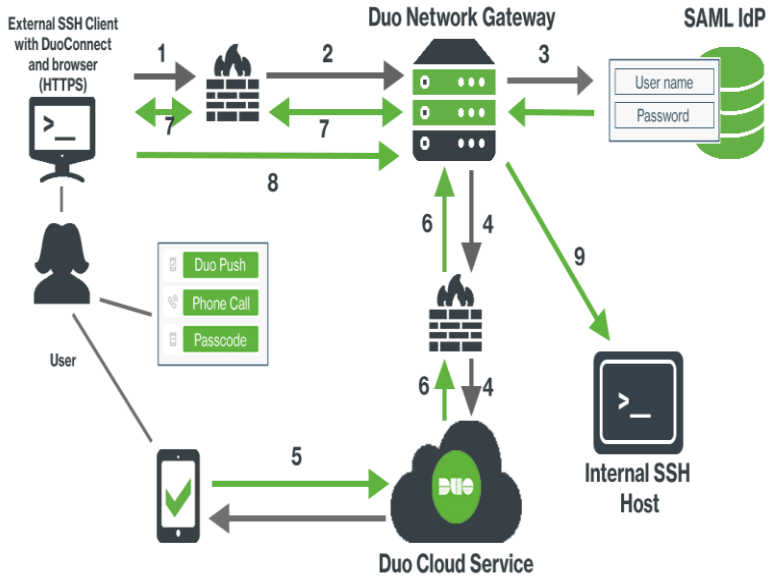

Figure 21: SSH server diagram [72]

In Fig 21,

1. The user starts SSH session and DuoConnect software on their computer and opens a browser window.
2. DuoConnect sends information over the user's browser to Duo Network Gateway over TCP port 443.
3. Primary authentication with username/password is completed via SAML identity provider standard. After correct input,
4. The Duo Network Gateway connection established to Duo Security over TCP port 443 and
5. Two-factor authentication takes place via Duo Security service.
6. The Duo Network Gateway receives and checks the authentication response.
7. Duo Network Gateway checks if DuoConnect is up to date and prompts if an update is available.
8. The DuoConnect connects the user's SSH session through Duo Network Gateway to the SSH server and
9. The user completes the regular SSH steps to access the application from any untrusted network. [72]

Features

- **User-friendly** - Duo 2FA is fast and easy for users to set up, and with several available authentication methods and the users can choose the one that best fits for their workflow. [73]
- **Several Token options** - The most used Duo token is push-based token through Duo mobile application. It also offers other token options like hardware U2F token (Duos D-100), SMS,

Phone calls, Time-based OTP. The new WebAuthn authentication option allows Duo 2FA login with in-built biometric login. [74]

- **Bypass code option** - This feature lets the administrator sets a manual code for a vendor or outside contractor for organizational access. This may also be handy in a situation where the user has forgotten their second-factor token at home or lost it. [75]
- **Easy scalability with Duo** - Duo functions as a gateway for your current and future IT infrastructure, it is the perfect solution for growing businesses. Set up new users and support new devices at any time and protect new applications instantly, without impacting legacy technology. [73]
- **Lightning-fast Deployment** - Duo can be added to any existing environment or platform and have a general deployment timeline blueprint for Duo rollout. Its self-enrollment feature makes it easy for users to get set up. [76]
- **Zero trust approach** - This approach builds trust for every device enrolled regardless of the location. It verifies the trust by checking that the users are using the corporate applications, device is corporate-managed, ensures device trustworthiness i.e. deny the request from any device that does not meet the required security level. Allows the admin to set policies and user roles to limit access to designated users only. [73]

Where Can Duo 2FA be used - It can be used to add a layer of security to Single Sign-on applications, websites, Custom applications, Active Directory Federation Services (ADFS), to protect your network login and for remote access authentication that are supported by Duo.

Maintenance - Duo follows an agile development cycle, issuing updates in hours and days in comparison to the several months and quarters, typical of the other 2FA vendors. The administrator does not have to install the updates manually as Duo updates the services automatically. The organization Administrator can with Duo Admin Panel can set policies like Fail-Safe - means if Duo service is unavailable, primary authentication access is granted or Fail-Secure - means no access without second-factor authentication. [77]
Another notable support is Duo status where you can check the operation service are running or not by giving you a Deployment ID (like DUO3, DUO10) and helps you identify the issues yourself.
They offer a set of Documentation for Administrator Panel overview, protecting applications, Enrolling users, for End-users and some other documental help which can be found at Duo.com's document page.
For troubleshooting Duo also offers some documents with testing steps and common issues solution which can be found at Duo.com's guide page.
Duo offers standard support and Duo Care+ (additional cost) for any technical issues support over the phone or Email 24X7X365 days for Duo Care+.

Security Standard - Meet compliance standards like PCI DSS, OWASP, ISO 27001, NIST 800 and more. [78]

Release Notes - The latest release note was published in October 2019, which means the developer is still updating and sending new patches for the product and solution.
Note - There may be latest updates released as this research was done at the end of 2019.
More information about the latest release notes can be found at Duo.com's release note page

Product license and pricing - Duo offers free trials for 30 days up to 10 users. Duo two-factor authentication is priced 3 USD for second-factor authentication, 6 USD for Duo Access and 9 USD for Duo Beyond per month. For more than 500 users you can contact Duo sales for a price quote. [79]

Uptime backed by Service Level Agreement - Ranges from minimum 95% to maximum 99.9% based on days and obligations met by customer. [80]

Security Features - Duo has Duo authentication proxy software that receives requests from local devices and applications through RADIUS or LDAP The Duo Authentication Proxy service communicates with Duo's service on TCP port 443. It has a support document for configuring various modes and options for RADIUS. [81]

Duo Beyond pack offers the organization with methods to monitor and identify risky devices, identify corporate-owned and BYOD devices, identify third party agent on the device enrolled, enforce policies based on authorized network, block anonymous networks, limit device access to the application set by administrator, unlimited applications can be integrated, secure remote access and enforce risk-based policies for authentication.
Antivirus - Device Health application antivirus/anti-malware agent confirms that the endpoints have one of these supported security solutions: Cisco Advanced Malware Protection (AMP) for endpoints, Windows Defender, Symantec Endpoint Protection, CrowdStrike Endpoint protection. Duo Device Health application evaluates a device to assess the status of its security and reports the findings of this scan to Duo. This helps Duo to keep the user device secure and improves problems that may occur before an authentication is needed. If this check reports an issue, such as the firewall turned off or OS out of date then it allows users to perform remedial measures before authentication. [82]

Lost Token?

If the self-service option is enabled and you have another token authenticated than you can log in with that option otherwise you to contact the admin either to delete you token from your account or to enable bypass code option for you to log in. Note- Bypass code expires after using and have a lifetime of 12 hours only. [83]

10.3 Yubico Yubikeys

Introduction

The Yubikey is a hardware device used as a second factor for authentication developed by Yubico. The YubiKey is a small USB and NFC device supporting multiple authentication and cryptographic protocols. With a simple touch, it protects access to computers, networks, and online services for the world's largest organizations. Yubikey provides strong two-factor authentication and supports FIDO2, FIDO U2F, one-time password (OTP), OpenPGP and smart card, choice of form factors for desktop or laptop.

Yubico offers different Yubikeys with different features named Yubikey 5 series, Security Key series, Yubikey FIPS series, Yubikey 5ci and working on YubiKey Bio which may be launched soon. [84]

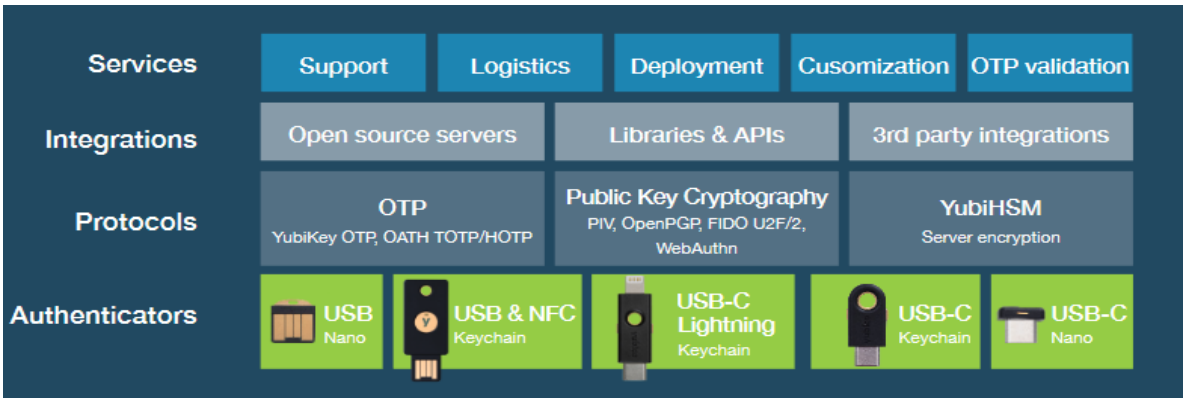

Figure 22: Yubico enterprise solutions [85]

Yubikey working with U2F

U2F method challenge-response protocol based on public-key cryptography which eliminates phishing and man-in-middle attacks. It consists of two flows: registration and authentication. It also offers applications specific keys, device attestation, and device cloning detection.

The U2F device has a private key k_{priv} and the relying party has corresponding public key k_{pub}. The keys are generated in a tamper-resistant execution environment.

For protection from Man-in-middle and phishing attacks, the U2F device verifies the origin of URI (Uniform resource identifier) which helps to mitigate the phishing attack and TLS channel ID to eliminate man-in-middle attack.

Application-specific keys will prevent the relying parties from tracking devices between different user accounts. This means that any website cannot know whether User1 and User2 share the same device. The U2F device creates a new key pair and key handle for each registration. The handle, h, is stored by the RP and sent back to the device upon authentication. This way, the device knows

which key to authenticate with, e.g. User1's key or User2's key. The key handle is stored by the server together with kpub. The App ID, a, is being used for scoping a key handle.

Yubikey keys cannot be read externally due to its tamper-resistant environment nature. However, to provide a clone detecting service to the U2F device without tamper-resistant secure elements (e.g. software implementations), the authentication counter is used. The device increments the counter when authenticating and the relying party verifies that the counter is higher than last time. The counter is sent from the U2F device to a relying party. [59]

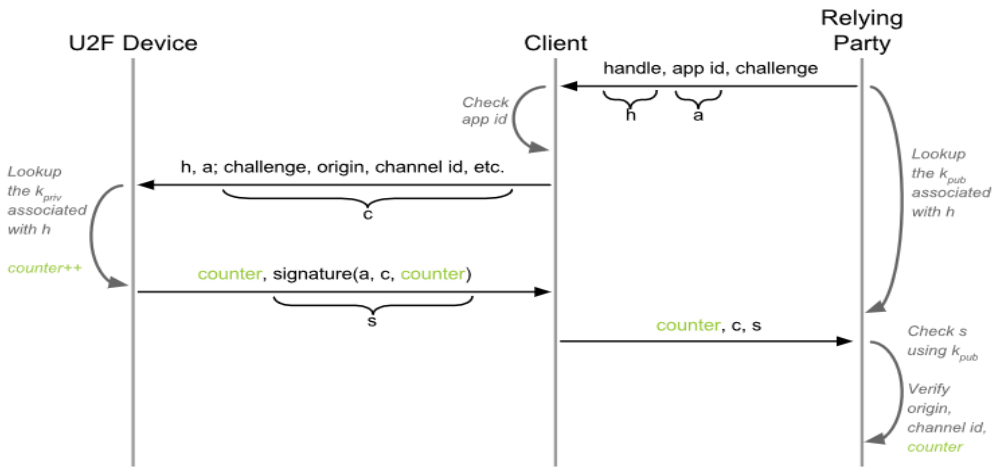

Figure 23: U2F technical diagram [59]

Verifying token properties from the relying party side is done by the Attestation concept. It is implemented via an attestation certificate which is signed by the U2F device and sent to relying party upon registration.

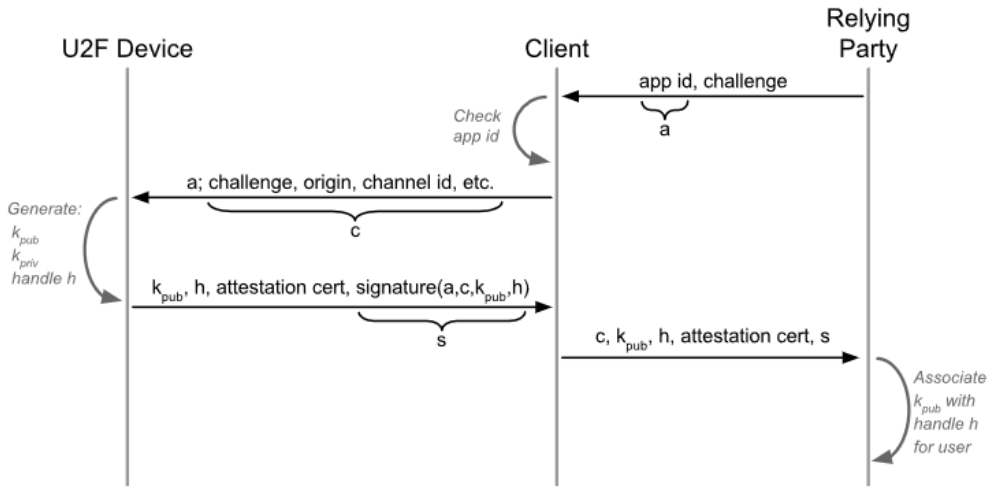

Figure 24: U2F technical diagram [59]

Yubikey with OTP

Another method offered by Yubico service is 44-character OTP, 128-bit encrypted Public ID, and password which is impossible to spoof easily. The OTP consist of two major parts, the first 12 characters are constant and represent the Public ID of the Yubikey device itself and the remain 32 characters are a unique passcode for each OTP generated. The validation is done from Yubicloud i.e. Yubico server and if your company does not want to use Yubicloud service then you can create your Verification server for validations of your users and employees. [86]

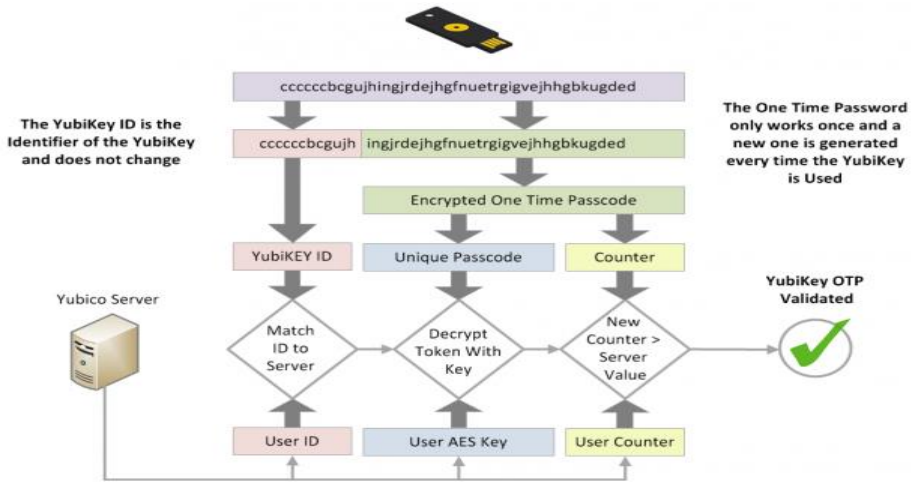

Figure 25: Yubikey OTP generation diagram [86]

Features & Benefits

- **Strong authentication** - Yubico YubiKeys are hardware authenticators as a second factor in addition to a password which is considered to be the strongest authentication method.
- **Different protocol options** - Yubikey Supports FIDO2, FIDO U2F, one-time-password (OTP), OpenPGP 3(Email) and smart card and they are working on the development of fingerprint authentication in-built in the Yubikey. [87]
- **Different Yubikeys -** They have Yubikeys of type-c for mobile support like YubiKey 5c**, Y**ubikey 5ci. Yubico offers Yubikey FIPS (Federal Information Processing Standards) series. YubiHSM 2 with dedicated hardware security module (HSM) and Yubico nono series Yubikey. These are also categorized for Individual or business use with distinctive features. [84]
- **Open source server** - Yubico offers developers with the Yubico OTP Validation Server and the Yubico U2F Validation Server to help facilitate the quick integration of the YubiKey functionality into an existing web site or service. Included is free open source software with the required source code and tools for web API clients, validation servers, and libraries. The validation software is offered as components for developers to integrate into any software or system. [88]
- **Open source tools** - Yubico offers open-source tools like Yubikey Manager, Personalization tools, Computer login tools, etc. for Windows, Linux and MAC OS. [89]
- **Remote access & VPN** - Yubikey can be deployed with RADIUS solution to facilitate remote access and VPN protection with second-factor authentication or you can use open-source code for building personalized Yubikey supporting remote and VPN access protection. [90]
- **One Key, multiple account** - Single YubiKey can be used for adding second-factor security for multiple accounts depending upon the credential capability of the YubiKey which can be found at Device options in Yubico website.

Where can Yubikeys be used - Yubikeys can be used for adding second-factor authentication security for web logins, computer login (Windows, Linux, MAC), for network login and Single-Sign-On applications.

Maintenance - Though Yubico offers a 1-year Yubikey warranty but there are other things to be taken care in an organization like the maintenance of all data and metadata, the maintenance of multiple local synchronized Yubikey Validation (YK-VAL) servers, maintenance of multiple local Yubikey Key Storage Module (YK-KSM) servers. [91] [92]
For enterprise administration control and reporting, you can integrate the Yubikey with keeper Business manager (costs additional). [93]
The YubiKey also enables secure privileged access management (PAM) which helps in protecting privileged accounts and improve the security of the organization. [94]

For basic troubleshooting of the Yubikey, you can visit https://demo.yubico.com for testing purposes and there are several basic troubleshooting documents available at Yubico support or else you can always create a ticket online for the issue for technical assistance.
Yubico support services tiers are Bronze, Silver, Gold and Platinum 24/7 to be chosen from respectively. The higher the tier level, the higher is the technical support and better response time. [95]
Antivirus - Yubico does not offer any anti-virus but Yubikey comes with privileged access management (PAM) that helps to protect privileged accounts and improve the security of the company.

Release Notes - The latest release note was published in January 2020 for yubikey-manager, which means the developer is still updating and sending new patches for the product and solution.
Note - There may be latest updates released as this research was done during 2019-2020. More information about the latest release notes can be found at Yubico.com's release note page.

Uptime backed by Service Level agreement - No, Yubico does not provide any up-time information.

Security Standards - YubiKey FIPS is validated by FIPS 140-2 and meets the highest authenticator assurance level 3 (AAL3) of NIST SP800-63B guidance. Other authentication standards include WebAuthn (W3C), OpenID and FIDO alliance. [96]

Product license and Pricing - YubiEnterprise subscription is a yearly or 3 years agreement as per user basis with a minimum purchase of 750 users. It reduces the ownership cost as it offers a per-user pricing model vs per-key pricing model. The users can even upgrade to new YubiKeys released. The price for YubiEnterprise can be requested from the vendor by completing an online form based on your requirements.
YubiKey 5 series price starts from 45$ USD, Security Key series price starts from 20$ USD, YubiKey FIPS series price starts from 46$ USD. Yubico offers volume discounts for YubiKeys ranging from 4% to 9%. [97]

Lost Token?

It is always recommended to have multiple second-factor authentication options. Or otherwise, try to use the recovery method supported by the website or application and de-associate the lost Yubikey from your account. If that is not possible, you must contact your administrator to de-associate or delete your key from your account. [98]

10.4 SafeNet Authentication Service

Introduction

SafeNet Authentication services provide a fully automated and highly secure authentication method with flexible token options like hardware, push notification or OTP as per your

organization requirements. Strong authentication. Strong authentication has been made easy through the flexibility and extensibility of SafeNet Authentication Service's automated workflows, vendor-agnostic token support, broad APIs, and seamless out-of-the-box integrations with over 300 solutions from leading brands. Without infrastructure requirement, SafeNet Authentication Service enables a quick migration to a multi-tier and multi-tenant cloud environment and protects everything, from cloud-based and on-premises applications to networks, users, and devices.
Example of SafeNet authentication integration with RADIUS AD of NetMotion company

On-premises of the organization - RADIUS agent that is implemented in the existing customer's RADIUS environment. The agent forwards the RADIUS authentication requests to the SafeNet authentication service cloud environment. The RADIUS agent can be implemented on a FreeRADIUS server only. [99]

Figure 26: SafeNet on-premises integration [100]

Cloud service - RADIUS service that is already implemented in the SafeNet authentication service cloud environment and can be used without any installation or configuration requirements. [99]

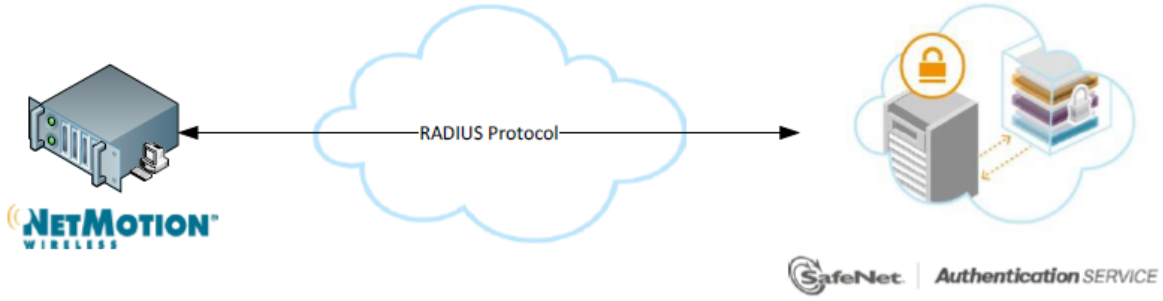

Figure 27: SafeNet cloud integration [100]

An example of User login from workstation depicting OTP two-factor authentication.

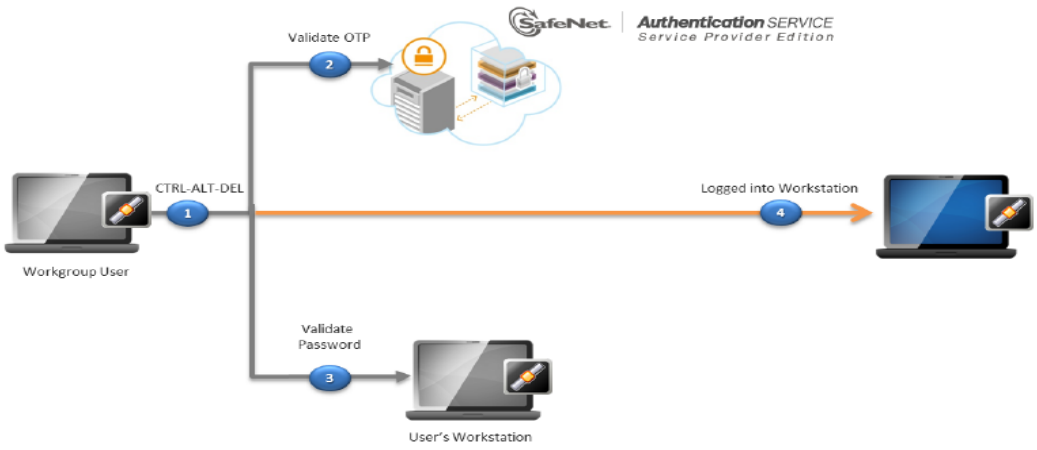

Figure 28: SafeNet workgroup authentication diagram [101]

In Figure 28, The user first presented with a SafeNet Authentication Service Windows login prompt and then click Ctrl+Alt+Del. Then the user enters their username. If the user is part of a local group, the credentials are passed to local workstation otherwise, the username and OTP are sent to for verification to SafeNet Authentication Service [101]
If the request is valid, the user is prompted to their Microsoft Password window. After entering the correct password, the user will be granted access to their workstation.

Below is the diagram depicting two-factor authentication solution, MobilePass+ push notification enabled in Microsoft office 365.
The enterprise enabled two-factor authentication for Microsoft office 365. The user enters the primary password and username and clicks the Sign-in button. The application sends the request to the server to identify the user and their mobile device. After this, the server will send the second factor push authentication to the user mobile. The user can tap on the notification to view the login request details and tap on the mobile device to allow access to Office 365 or deny the request in the case where the login request is not genuine. [102]

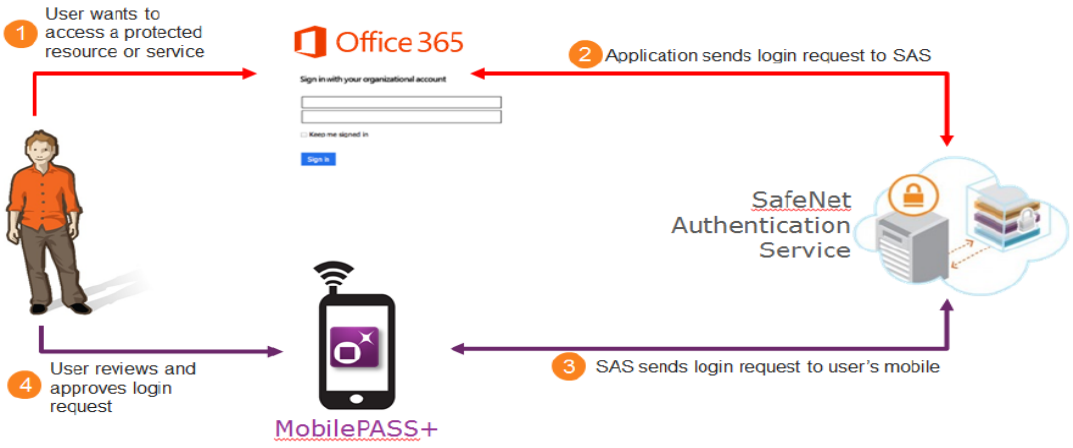

Figure 29: SafeNet push authentication flow diagram [102]

SafeNet Authentication Service Delivery model for Enterprise

SafeNet Authentication Service (SAS) is an enterprise-class authentication server designed to expand the authentication services to users in a single organization or throughout an unlimited number of individuals. These entities can be anything, from divisions or cost centers within a company, to subsidiaries or completely independent organizations. Its multi-tier, multi-tenant structure accommodates just about any hierarchy, reporting structure or organization structure to enable two-factor authentication and other services provided by SafeNet. [103]

The SafeNet offers Software-as-a-Service (SAS) authentication platform with 24/7 availability and no hardware requirements. The SafeNet experts manage the security task which relieves the organization from supervising security checks. Using one cloud-based platform to manage, maintain, and provide a wide range of tokens, SAS can grow with your organization's requirements and ensuring security to the endless number of users in a wide range of token form factors. SafeNet also offers Service Provider Edition (SPE), a cloud-based authentication management service for your organization and the organization wanting to create an on-premises authentication management solution can opt for Private Cloud Edition (PCE) by SafeNet. [103]

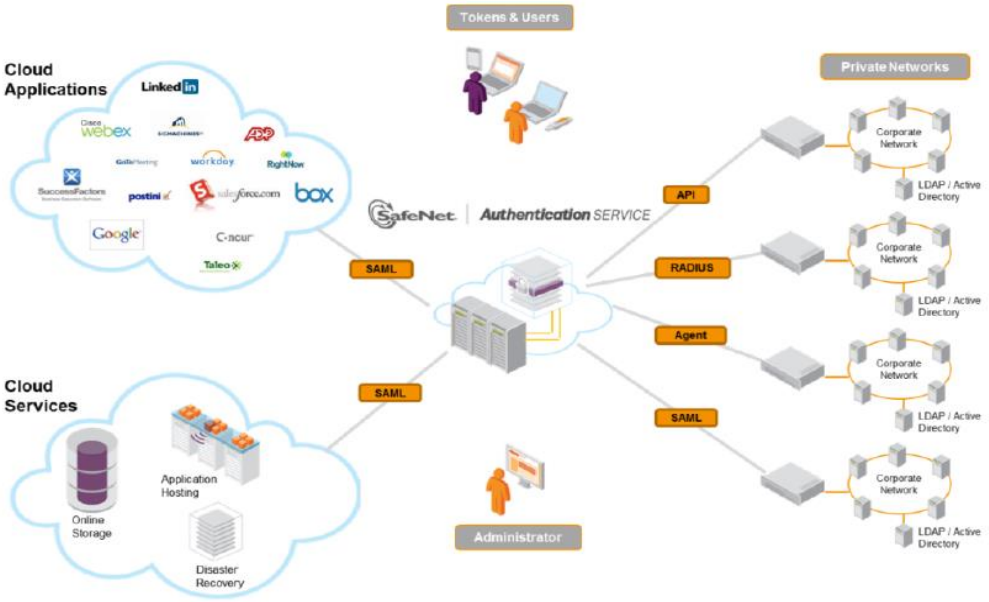

Figure 30: SafeNet authentication service working [104]

Feature and Benefits:

- SafeNet Authentication Service proves that high security does not have to mean high costs and high maintenance.
- SafeNet Authentication service can work with the existing technology of the organization and migrate fast with the help of a migration agent. [105]
- **Fast Deployment** - The SafeNet Authentication can authorize and allocate 20,000 users in just 20 minutes. Increase the productivity of the organization. [105]
- **Cloud-based** - It also reduces the deployment cost as there is no need to install any additional hardware server for implement SafeNet service and provide full automated lifecycle administration of user permissions, automatic updates and automatic reporting features and alerts which reduces IT overhead management cost. [105]
- **Scalable** - It offers easy scalability to an unlimited number of users for future growth. [105]
- **Policies** - As an administrator, it gives you the power to set policies and authentication levels according to user needs to enhance security. [105]
- **Automated provisioning and management** - Offer self enrolment provisioning for users to save administration time, allows bulk pre-allocation and de-allocation of any token type for a group via group-policies function. [105]

- **Price-per-user model** - SafeNet authentication uses price per model to provide better insight into pricing according to your organization's needs. This price also includes migration and access agent and management console. [105]
- **Automatic reporting** - This reduces the resources required otherwise to create and take actions on the risk reports. SafeNet also offers a ready-made reporting template according to organization needs and allows you to customize the template as well. [105]
- **Security** - SafeNet authentication service is a risk-based authentication and allows us to set pre-authentication rules via the admin console. For example, admin can set block logins for a time in a day, allows authentication agent, restrict certain IPs to login to corporate network and has some other properties which enhance the security measures provided by SafeNet. This isn't quite as competent as some of its competitors, but at least a beginning attempts at recognizing that some customers will want more restrictive policies. [103]

Where can SafeNet authentication service be used - SafeNet authentication can be used for VPN logins, local network login, Single sign-on applications, and website logins.

Maintenance - SafeNet offers an Authentication client, which is a desktop-based software for PKI-based authentication management. This software helps to guarantee the full support for all currently deployed tokens and enables local administration of the devices, client customization, setting policies, network access management and much more. [106] SafeNet has provided documentation for integrating second-factor login for VMware and web application thoroughly which can be used by IT staff for management and deployment.

SafeNet Authentication Service also includes workflow automation and management tools that can decrease the deployment and management costs to near zero. For instance, by combining LDAP synchronization with provisioning rules, each time your account adds a user in their LDAP server, within minutes SafeNet authentication service will automatically create the user account in their Virtual Server and provision the user with a token and all of this is done without your staff clicking a mouse button. You can refer to the SafeNet Authentication Service provider authentication guide for detailed steps configuration integration. [103]

Troubleshooting - Some basic troubleshooting questions are explained in the documentation or else you can create an online ticket for your issues on the 24X7 web portal or call them on regional number. [107]

Security Standard - SafeNet authentication service meets FIPS 140-2 validated software and hardware tokens, ISO 27001:2013 accreditation, DSKPP-secured provisioning of software tokens AND ANSSI certified libraries within software tokens. [108] [109]

Release Notes - The latest release note was published in October 2019, which means the developer is still updating and sending new patches for the product and solution.
Note - There may be latest updates released as this research was done at the end of 2019.

More information about the latest release notes can be found at SafeNet.com's release note page.
Product license and cost: SafeNet offers a yearly subscription with 250-499 license volume and 3-year subscription with 1000-2499 license volume. The yearly cost for 100 tokens if 1200$ USD. [110] [99]

Uptime backed by Service Level Agreement - Gemalto's warranty for production instances is no less than 99.99% Monthly Uptime Percentage for cloud services and SafeNet authentication service with an uptime percentage of 99.99999%. [111]
Note - Monthly Uptime percentage is calculated as the total number of minutes in a calendar month minus the number of minutes of Downtime suffered from all downtime periods in a calendar month, divided by the total number of minutes in a calendar month

Lost token?

The organization administrator can customize the SafeNet web portal for sending temporary token links. Links can be sent on user authenticated information and the lifetime of link can be set by the administrator. [112]

10.5 SecurEnvoy SecurAccess

Introduction

SecurEnvoy company provides security solutions by taking advantage of using mobile and Secure access technology to provide phone-based two-factor authentication. The secure access technology can enable two-factor authentication for corporate networks on-premises or on cloud. They offer an easy integration with the existing LDAP of the organization without the requirement of creating a new user database. The user can choose any of their device to be their authenticator token like soft token App, SMS option, laptop, or any smart wearable. Secure access offers various interfaces to support on-premises application 2FA, SaaS 2FA or network connectivity 2FA (Secure Ice license).

SecurEnvoy secure access offers two topologies: Internal server topology i.e. no internet facing web portal and Internal server topology with web resource. In the internal server topology, the only attack risk is from inside the organization and it reduces the server hardening cost while the other topology service is accessible to internet users and needs good server security. Below is the internal server topology diagram that can be used to authenticate VPN users with the second-factor or to add the second-factor to organization application etc. and the user would be required to be on the corporate private network to manage their tokens while the other topology, the user can manage their token from anywhere without needing to be connected on corporate private network or through the network.

The diagram for other topology is slightly different as it just shows the users are connecting through the internet. LDAP connection concept is the same. [112]

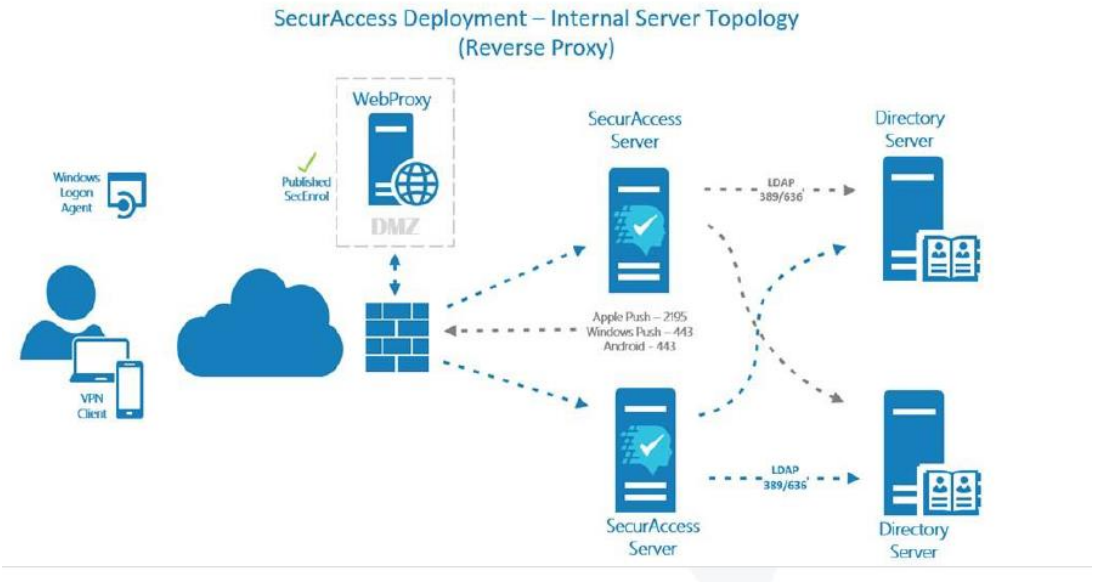

Figure 31: SecurAccess integration diagram [112]

Benefits & features

- **Deployment option** - SecurEnvoy offers on-premises software or hosted via managed provider service for enterprise according to budget fit. [113]
- **Automatic group deployment** - SecurAccess easily integrates with Active Directory of the organization and offers selection and control through the self-enrollment portal for automated group deployment. This reduces the IT staff overhead and can deploy 100,000 users per hour. [113]
- **Authentication option** - User adoption is one of the main factors for implementing any new solution in any area. SecurAccess give users the option to choose security token based on their convenience like mobile phone, laptop, wearable, SMS or push notification. [113]
- **SecurAccess Security Virtual Appliance (VSA**) - VSA facilities easy trial, demonstration, and deployment at the enterprise level for small, medium, and large organizations. This is based on Microsoft server 2016 which was designed to stack and scale in multiple configuration by supporting easy scalability and flexibility. [114]
- SecurAccess utilizes the existing Active directory of the organization to save costs. [113]

Maintenance - SecurEnvoy SecurAccess offers easy mass deployment with an automatic group deployment feature within the admin GUI. This feature facilities the ongoing automatic provisioning of the users which reduces admin tasks and management. The dedicated for automatic group deployment is called the Deployment Wizard. SecurEnvoy Batch server checks the users in organization AD and sends the new second-factor code.

It supports various domains such as Microsoft AD, open LDAP, SUN directory server and Microsoft LDS giving organization option to choose concerning prerequisite knowledge. SecurEnvoy SecurAccess can be employed based on a single server or multi-server approach and a multi-server provides the redundancy level reducing the failure management risk. The SecurEnvoy Administration and configuration guide provide detailed insight into the implementation and management of the solution. [115]

Troubleshooting - SecurEnvoy SecurAcces have enough detailed integration document to search for known issues. Apart from that, the Report Wizard tool provide administrator for investigation of user and overall system. It provides various options to view all managed users, disabled users, Enabled users, Day code users, Real-time OTP user's vs Preload OTP users and much more for sighting risk. You can also reach the SecurEnvoy technical team after filling online form with issue details. [115]

Release Notes - The latest release note was published in February 2019 and before that was published in July 2018. The latest updates are done yearly.
Note - There may be latest updates released as this research was done at the end of 2019. More information about the latest release notes can be found at SecurEnvoy.com's release note page.

Security - All stored authentication data is generated and encrypted with AES 256-bit encryption and is kept within the customer LDAP server. SecurEnvoy Security server provides a wide range of web portals like admin console, Token portal, SecurPassword portal, SecurMail Sender portal, etc. to give the administrator wide power to choose from. Some other features which are included in SecurEnvoy server it that it automatically deletes the used passcode from the system to eliminate the risk of replay attack on any user and this is known as Watermarking. It also gives you the feature to set up real-time email alerting for better protection and risk assessments.
Antivirus - It does not come with any in-built anti-virus protections. It is recommended to use your update antivirus version. [115]

Uptime backed by Service Level Agreement (SLA) - Ranges from 90% to 95% maximum every month. [116]

Lost token?

SecurEnvoy comes with a self-help desk web portal that can help the users in the situation of lost or stolen tokens. [103]

10.6 Glimpse at other 2FA solutions

Google authenticator is a 2FA solution created for a single user or a small business. It provides a medium to securely authenticate users with the help of TOTP (Time-based one-time password) service. To make this service run it needs access to the camera to scan the QR code. It does not provide authentication services like single sign-on and identity management. That is the reason it is not widely used within the business community for the fact that the user must use the authenticator each time the user wants to use a different application.

Other authenticators like RSA Secure ID and Ping Identity uses technology like Identity Access Management and SSO (Single Sign-On) which is helpful in large enterprise network environments. Multiple vendors provide different services with their 2FA solutions. For example, Ping Identity provides Identity and Access Management, passwordless authentication, Privilege access management, etc. and RSA secure ID provides SSO with Biometric authentication. Useful features inclusion comes with a price hence the solutions are based on per-user pricing for any organization. Solutions like Privilege access management works on the principle of Role-Based Access Control and provides multi-level access apart from authentication which enriches the implemented 2FA solution with useful services

11: Two-factor Authentication Is Not Enough

The two-factor authentication solution was designed to add an extra layer of security to a user account. However, hackers have found ways to bypass the second factor of authentication to access the user accounts for malicious purposes. Hackers may now use a type of phishing techniques to get around two-factor authentication, typically a code sent your cellphone that is needed to log in or even bypass the second factor with the help of social engineering techniques. There is no ideal solution to security.

11. Various technique to bypass 2FA authentication:

Man-in-the-middle attack - Man-in-the-middle (MitM) attacker can fool you into visiting their fake website through email or text message and prompt you for your 2FA credentials, it's essentially game over. The MitM attacker can fake a website that you trust where you are using the 2FA and subsequently fool you into to reply to a prompt and steal your 2FA credential. If the hacker gained access to your account by bypassing 2FA, there is nothing to stop him from changing the phone number the next code will be sent to or steal your data. Hackers may also use IP spoofing to catch communication packets between two parties. [117]

Social Engineering - One of the most common techniques is SIM swapping. An attacker can impersonate you and request your network provider to change the phone number to a new phone in a phone number porting fraud. NIST Special Publication 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management. NIST has stated: "Due to the risk that SMS messages may be intercepted or redirected, implementers of new systems SHOULD carefully consider alternative authenticators and does not recommend using this type of second-factor authentication in their guidelines. [118]

Password reset - 2FA can also be bypassed using 'lost password' privilege to recover the user account. For example, if the hacker has gained access to your email account and the account is linked to other sites for backup then the hacker can use the 'Forgot password' option to get the 'Reset password' link in your email inbox. However, this is a rare case.

Brute force - Usually the second-factor secret code is a 4 to 6-digit number or limited character combination. If the website does not have a suitable rate-limiting method to control the amount on the incoming request, then the second-factor code is vulnerable as the attackers have enough time to apply brute force to your second factor. However, this may be a rare case as Time-based OTP (TOTP) are commonly used which has 30 seconds of limited validity.

Organization should avoid simple 2FA methods such as SMS 2FA or OTP codes (use TOTP instead). The adopted 2FA solution should have capabilities to control adaptive access to balance the level of trust for the incoming login request and does risk analysis based on the situation providing a better security paradigm for the organization.

For example, the administrator should be able to set policies to block any non-standard geographic location request or request that is coming from non-corporate IP. Should grant only trusted device access to corporate networks.

Organization should also provide Security Awareness Training to its employees once every year to provide a better insight for known malicious activities and what to do in those situations.

In the next section, we will cover next-generation solutions or techniques for providing authentication rather than just two-factor authentication. [119]

12: The search for the better

12.1 Multi-Factor Authentication (MFA)

Multi-Factor authentication is an authentication system that requires two or more authentication factors from the user to access their account. Two-Factor authentication is a subset of a multi-factor authentication system that requires the user to provide a combination of two credentials: what the user knows (passwords), what the user has (security token) and what the user is (biometrics).

The organizations can even implement a three-factor authentication (3FA) system to enhance the authentication level security. It will be highly unlikely for any hacker to possess all three factors of authentication to hack into someone's account.

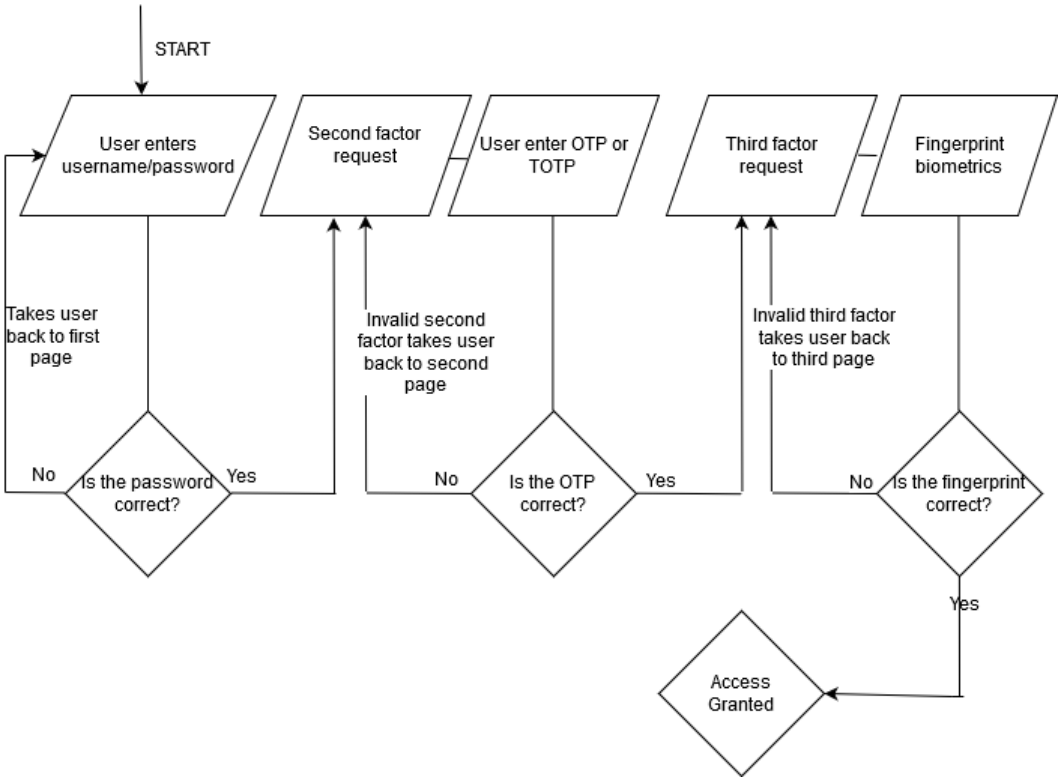

Figure 32: Three-factor authentication flow diagram

Pseudocode of the above model

```
Start
Input username
Input password
IF Username & password are correct THEN
        Proceed to second-factor authentication
```

```
ELSE
        Print Id or password incorrect
        IF unsuccessful attempts = 5
                alert user registered mobile or email and administrator
        Return to try again
Input OTP or TOTP
IF OTP is correct THEN
        Proceed to third-factor authentication
ELSE
        OTP or TOTP code incorrect
        IF unsuccessful attempts = 3
                alert user registered mobile or email and administrator
        Return to try again
Input Fingerprint Biometrics
IF Fingerprint is correct THEN
        Access Granted
ELSE
        Fingerprint is invalid
        IF unsuccessful attempts = 2
                alert user registered mobile or email and administrator
        Return to try again
End
```

Similarly, the above model can be modified to four-factor authentication or more factors. However, the more authentication factors, the more complex it will be to use and integrate into your organization. Three-factor authentication is recommended for an extremely prominent level of data security. It is not recommended for daily use applications as it will increase the login time and will act as a barrier between the users and application. The more factors for the authentication method can also be costly and time consuming for any organization.

Users consider the second-factor authentication or multifactor authentication as an inconvenient authentication method as it increases the login time for the users and affects the usability.

Figure 33: Search for better [120]

12.2 Passwordless Authentication

Passwordless authentication is a type of Multifactor Authentication (MFA). It eliminates the commonly used username/password method and provides faster and easier authentication means for the users. Instead of entering a password for authentication, the passwordless authentication authenticates the user based on possession of something the user has, for example, a one-time password generator, a registered mobile device, or biometrics input.

Passwordless authentication eliminates the attacks related to password hacking. It provides better security, better user experience, fast login and reduction in total cost of ownership for password management. [121] Password-less authentication would make it possible for more users to adopt a service as they would be able to access a system with more security and minimal friction. This could lead to a spike in the customer acquisition rate that organizations currently may have challenges with. Remembering complex passwords that change every so often is a challenge.

Passwordless authentication technology is like digital certificates. It uses cryptographic key pairs that include public and private keys. A private key is stored on the local device of the user and linked to an authentication factor like a PIN, fingerprint, or face recognition. The public key, on the other hand, goes to the website or application where the user wishes to log in.

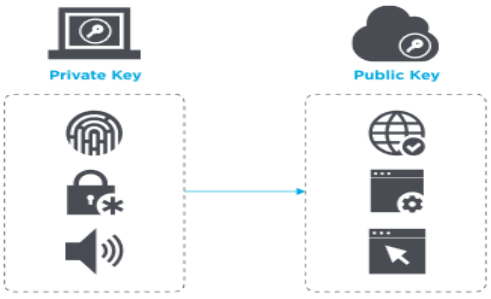

Figure 34: Passwordless authentication key elements [122]

List of different passwordless authentication software and technologies: Yubico passwordless with Microsoft azure, Authentiq, BlockId, HYPR Corp., Auth0 passwordless, Windows Hello (for window 10), Duo TouchId and many more are available on the internet.

The FIDO (Fast IDentity Online) Alliance is an open industry association whose aim is to develop and promote authentication standards that help lessen the world's over-dependence on the passwords.

FIDO2 project - Moving the World Beyond Password

The FIDO2 Project is a joint effort between the FIDO Alliance and the World Wide Web Consortium (W3C) whose goal is to create strong authentication for the web.

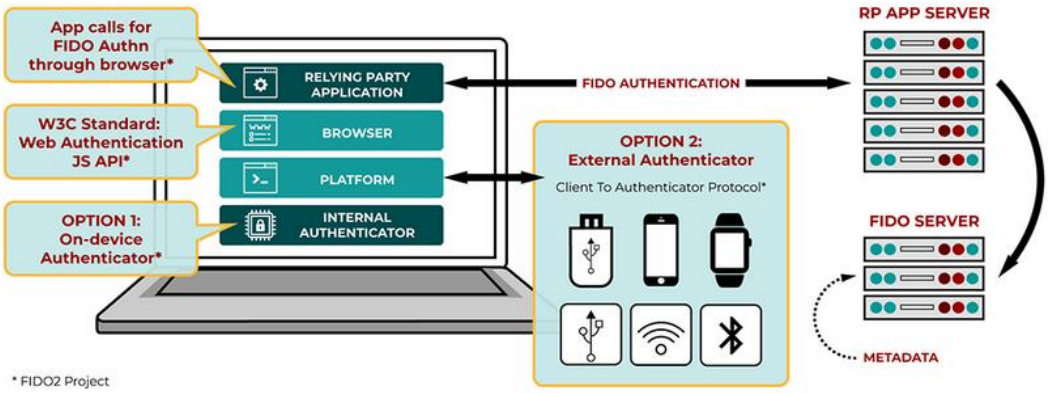

Figure 35: WebAuthn flow diagram [123]

FIDO2 project consists of W3C WebAuthn standard is implemented on the client browsers as an API which enables the support for FIDO authentication. The client to authenticator protocol (CTAP) allows the use of external authenticators like FIDO keys for authentication on FIDO2-enabled browsers and operating systems over biometrics, USB, NFC, or BLE for a passwordless, second-factor or multi-factor authentication experience. This protocol also supports internal.

FIDO universal authentication framework (UAF) protocol supports a passwordless experience. With FIDO UAF, the user carries a device with a FIDO UAF stack installed. The user can register with an online service that supports FIDO2 standard and generates a new key pair, public key - registered in the online service database and a private key- stored on local devices. After the process is completed, the user can now authenticate themselves with a password using the private key stored in their device by pairing it with the public key stored in the web services. [123]

For example, the Windows 10 users can enable the new authentication feature on the windows known as 'Windows Hello', the passwordless authentication method using biometrics information and it is FIDO2 certified as well. "Hello for Business is personal, simple, and provides a brilliant user experience with high security. Our people love logging on with their fingerprint face.

Password-less protection-Peter Scott," Director of Dynamic IT, British Telecom Technology. [124]

Multi-factor authentication method, passwordless authentication is going to continue to evolve. Most organizations still use traditional passwords as their core authentication method. But the broad and known problems with passwords are expected to increasingly drive businesses using Identity Access Management toward Multifactor authentication options and toward passwordless authentication.

13: Conclusion

According to the above study, SafeNet Authentication Service (SAS) is the cheapest solution for implementing two-factor authentication in any organization which will cost only 1$ USD per month per user. Its cloud nature reduces the IT cost of implementing new server and management and it gives the administrator the power to set automatic group provisioning which saves a lot of money. Also, SafeNet can be This solution support Email, SMS, mobile and hardware token.

For users, SafeNet has enough detailed API integration document available for installation. This is another plus point as it may reduce the installation IT cost. SafeNet offers authentication client for easy monitory and reporting, workflow automation and management tools that can decrease the deployment and management costs to near zero. The uptime SLA backed of SafeNet is 99.99999% which is the highest availability among other two-factor solutions. SafeNet offers the right number of features and prices for providing two-factor authentication solution.

SafeNet has a lot of integration guides covering how to integrate with Google Docs, Cisco VPNs and numerous other products using SAML and SOAP protocols, and these documents are available to anyone online. Which gives it a heads up for any organization to opt for it as a second-factor solution.

For best security solution option, I would recommend Duo 2FA. Security is a top-level concern for every company, and they are willing to pay a lot of money for it. Duo provides the best security regarding second-factor authentication. Its price ranges from 3$ USD (basic plan) to 9$ USD (many features). Known as Duo Beyond, comes with a lot of features to protect user account such as it gives the administrator to monitor the risky devices, security health of laptops and desktops with Duo health application.

It also supports Bring Your Own Device policy. Duo has well-documented API integration and Admin API document for ease of deployment and management, but It may require technical support while installation. It allows the administrator to set policies per user group or globally enforce security as per applications. It gives you multiple options to choose from while selecting your second factor of authentication.

Another recommendation, Duo also supports U2F keys i.e. Security keys which are providing the highest security as compared to other forms of factors like SMS, Emails, OTP, etc. They do cost additional but if you want to protect high-level data then Duo Security Keys combined with Duo security features delivers a strong pack of providing two-factor authentication.

Two-factor authentication adoption rate is increasing tremendously among users and businesses. It is the best type of security option available nowadays. The added security makes the account more resilient and it has saved many organizations and users from online attacks. There are dozens of free and paid 2FA solutions available according to the user needs.

There has been research on the global market trends which believe that the 2FA market value is expected to reach USD 8,984 million and is expected to grow at a 17.28% compound annual

growth rate by 2024. [125] The primary password/username method will stick around for a while with an added layer of security provided with 2FA or MFA.

However, Passwordless authentication is the next step in the authentication market. Users consider it easier to use and faster than the MFA authentication method. The new devices in the market are already equipped with biometric sensor capabilities. This allows the user to choose the easier and better authentication method known as "Passwordless authentication." For example, modern technology for fingerprint reader allows users to set biometric authentication for their account which is considered as the most secure method.

"Windows Hello," which is another example of Passwordless authentication allows the user to login into their device using facial recognition or fingerprint. It also enables you to use your digital wristband, smartwatch, phone, and other devices to quickly unlock your Windows PC without using a password. Passwords

In gist, the Passwordless authentication could be a potential turning point in the authentication methodology. Many organizations are moving towards Passwordless authentication systems and many others will follow the same suite, until than MFA or 2FA will rule the market trends

Bibliography

[1] A. Barbir, "FIGI Secuirty Clinic," 2019. [Online]. Available: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201912/Documents/Amy%20Ulrich.pdf.

[2] "Authentication," [Online]. Available: https://en.wikipedia.org/wiki/Authentication.

[3] A. Ometov, N. Makitalo, Y. Koucheryavy, "Multi-Factor authentication: A Survey," 2018. [Online]. Available: https://www.researchgate.net/figure/Conceptual-authentication-examples_fig1_322288752.

[4] "Authentication," [Online]. Available: https://en.wikipedia.org/wiki/Authentication.

[5] "Retinal scan," [Online]. Available: https://en.wikipedia.org/wiki/Retinal_scan. [Accessed 2019].

[6] L. Blabas, "Digital authentication - factors, mechanisms and schemes," [Online]. Available: https://www.cryptomathic.com/news-events/blog/digital-authentication-factors-mechanisms-schemes.

[7] J. Clement, "Global Digital Population," [Online]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/.

[8] R. Picheta, "The most commonly hacked passwords, revealed," 07 February 2019. [Online]. Available: https://www.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html.

[9] “15 Alarming Cyber Security Facts and Stats,"September 2019. [Online]. Available: https://www.cybintsolutions.com/cyber-security-facts-stats/.

[10] "40 Scary Hacking Statistics that Concern Us All in 2020," [Online]. Available: https://hostingtribunal.com/blog/hacking-statistics/#gref.

[11] N. Sharma and M. Farik, "Security Gaps in Authentication," [Online]. Available: https://www.researchgate.net/publication/311513572_Security_Gaps_In_Authentication_Factor_Credentials.

[12] C. Nachreiner, "Digital authentication: The past, present and uncertain future of the keys to online identity," 13 September 2018. [Online]. Available: https://www.geekwire.com/2018/digital-authentication-human-beings-history-trust/.

[13] "Understanding Password Authentication & Password Cracking," [Online]. Available: https://www.wordfence.com/learn/how-passwords-work-and-cracking-passwords/.

[14] I. solutions, "The History of Digital Authentication," October 2019. [Online]. Available: https://www.ictsolutions.co.uk/the-history-of-digital-authentication/.

[15] "Single Factor Authentication," [Online]. Available: https://searchsecurity.techtarget.com/definition/single-factor-authentication-SFA.

[16] I. Degtiarenko, "What are the top 10 viruses of all times?," MacPaw, 19 Feburary 2019. [Online]. Available: https://macpaw.com/how-to/top-computer-viruses-of-all-times.

[17] A. Goodman "Secure Access for the Digital Enterprise," August 2018. [Online]. Available:https://www.pingidentity.com/en/company/blog/posts/2018/five-preventable-breaches-make-the-case-for-mfa-everywhere.html.

[18] "Phishing: How many take the bait?," Get Cyber Safe / Pensez cybersécurité, 2015 March 2015. [Online]. Available: https://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx.

[19] "2017 Annual Threat Report," eSentire, February 2019 [Online]. Available: https://www.esentire.com/blog/esentire-threat-landscape-and-forecast-for-2017-and-2018-overview

[20] J. Vijayan, "SQL Injection Attacks Represent Two-Third of All Web App Attacks," 2019. [Online]. Available: https://www.darkreading.com/attacks-breaches/sql-injection-attacks-represent-two-third-of-all-web-app-attacks/d/d-id/1334960.

[21] M. Mayne, "XSS turns 2019's most popular cyber-attack," [Online]. Available: https://www.scmagazineuk.com/xss-turns-2019s-popular-cyber-attack/article/1669609.

[22] "Password Cracking," [Online]. Available: https://en.wikipedia.org/wiki/Password_cracking.

[23] Graphus, "Social Engineering Likely Cause of Yahoo! Hack," [Online]. Available: https://www.graphus.ai/social-engineering-likely-cause-of-yahoo-hack/.

[24] Mark Stanislav, Two-Factor Authentication, IT Governance Publishing, 2015. ISBN 978-1-84928-734-0: O'Reilly Media, Inc.

[25] K. Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," 4 June 2017. [Online]. Available: https://www.wired.com/2010/01/operation-aurora/.

[26] S. Larson, "Every single Yahoo account was hacked," 4 October 2017. [Online]. Available: https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html.

[27] N. Hopkins, "Deloitte hit by cyber-attack revealing clients' secret emails," 25 September 2017. [Online]. Available: https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails.

[28] Timehop, "Security," [Online]. Available: https://www.timehop.com/security.

[29] "Multifactor Authentication," [Online]. Available: https://en.wikipedia.org/wiki/Multi-factor_authentication.

[30] "What is Two Factor Authentication: Pros and Cons of 2FA: Imperva," [Online]. Available: https://www.imperva.com/learn/application-security/2fa-two-factor-authentication/.

[31] E. Huseynov &. J-M Seigneur, "Pervasive two-factor authentication using Wi-Fi SSID broadcasts," [Online]. Available: https://www.researchgate.net/figure/Classic-two-factor-authentication-flowchart_fig10_283489178.

[32] L. Harbaugh, "Two-Factor Authentication: Solutions, Methods, Best Practices," August 2018. [Online]. Available: https://www.msp360.com/resources/blog/two-factor-authentication-solutions/.

[33] "Time-based One-time Password algorithm," [Online]. Available: https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm.

[34] "A guide to common types of two-factor authentication," September 2017. [Online]. Available: https://venturebeat.com/2017/09/24/a-guide-to-common-types-of-two-factor-authentication/.

[35] "FIDO Alliance," [Online]. Available: https://fidoalliance.org/specifications.

[36] "Specifications Overview," [Online]. Available: https://fidoalliance.org/specifications/.

[37] "Universal 2nd Factor," [Online]. Available: https://en.wikipedia.org/wiki/Universal_2nd_Factor#Support_and_use.

[38] "two-factor authentication (2FA)," [Online]. Available: https://searchsecurity.techtarget.com/definition/two-factor-authentication.

[39] "Zero Trust Security for the Workforce," [Online]. Available: https://duo.com/use-cases/industry-solutions/zero-trust-security.

[40] "4 key benefits of Two-factor authentication to protect your data," [Online]. Available: https://www.pointclick.net/4-key-benefits-two-factor-authentication-2fa-protect-data/.

[41] P. Grassi, M. Gracia & J. Fenton"NIST Special Publication 800-63-3," June 2017. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3.html.

[42] Micheal, "Top 2020 Banking Regulations & Security Compliance Requirements," [Online]. Available: https://www.onespan.com/blog/top-banking-regulations-security-compliance-requirements.

[43] J. Rains "HDI," May 2012. [Online]. Available: https://www.thinkhdi.com/library/supportworld/2011/password-reset-practices.aspx.

[44] "What Are the Benefits of Two-Factor Authentication?," [Online]. Available: https://messente.com/blog/most-recent/benefits-of-two-factor-authentication.

[45] S. Frazier, "The 2019 State of the Auth Report: Has 2FA Hit Mainstream Yet?," December 2019. [Online]. Available: https://duo.com/blog/the-2019-state-of-the-auth-report-has-2fa-hit-mainstream-yet.

[46] " 3 disadvantages of two-factor authentication," October 2017. [Online]. Available: https://www.electronicproducts.com/Programming/Software/3_disadvantages_of_two_factor_authentication.aspx.

[47] J. Rossignol, "Apple Faces Yet Another Class Action Lawsuit Over 'Secretly Throttling' Older iPhones," August 2019. [Online]. Available: https://www.macrumors.com/2019/08/01/iphone-throttling-lawsuit/.

[48] S. Carter, "The Challenges and Benefits of Multi factor Authentication - MFA 101, Part 2," June 2017. [Online]. Available: https://blog.identityautomation.com/the-challenges-and-benefits-of-multi-factor-authentication-mfa-101-part-2.

[49] "Two-Factor authentication Evaluation guide , from Duo" [Online]. Available: https://duo.com/resources/ebooks/two-factor-authentication-evaluation-guide.

[50] "Guidance and Resources," June 2006, Version 1.0, ISBN 0-478-24466-5[Online]. pp 33-36 Available:https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/assets/Uploads/Documents/egif-authentication-multi-factor-guidance-june-2006.pdf

[51] N. Arboleda, "Government proposes tighter telco porting rules to fight scammers," October 2019. [Online]. Available: https://www.crn.com.au/news/government-proposes-tighter-telco-porting-rules-to-fight-scammers-532436. [Accessed 2019].

[52] N. Chakraborty, "Multi-factor authentication: A security layer," 5 March 2019. [Online]. Available: https://www.livemint.com/money/personal-finance/multi-factor-authentication-a-security-layer-1551722691516.html. [Accessed 2019].

[53] "2-step Verificatiom," [Online]. Available: https://home.dotgov.gov/2step.

[54] "Guidance and Resources," June 2006, Version 1.0, ISBN 0-478-24466-5[Online]. pp 33-36 Available:https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/assets/Uploads/Documents/egif-authentication-multi-factor-guidance-june-2006.pdf

[55] K. Thomas & A. Moscicki "New research: How effective is basic account hygiene at preventing hijacking," May 2019. [Online]. Available: https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html.

[56] T. Norris, "The Case for Multi-Factor Authentication Wherever Users Connect," August 2018. [Online]. Available: https://www.csoonline.com/article/3296011/the-case-for-multi-factor-authentication-wherever-users-connect.html.

[57] D. Storm, "Three examples of multifactor authentication use cases," [Online]. Available:https://searchsecurity.techtarget.com/feature/The-fundamentals-of-MFA-The-business-case-for-multifactor-authentication.

[58] "Case Studies, GOV.UK" [Online]. Available: https://www.yubico.com/resources/case-studies/.

[59] "U2F Technical Overview," [Online]. Available: https://developers.yubico.com/U2F/Protocol_details/Overview.html.

[60] "National Cyber-Forensics & Training Alliance (NCFTA): Duo Case Study," [Online]. Available: https://duo.com/use-cases/case-studies/national-cyber-forensics-and-training-alliance-ncfta.

[61] "Stinson Leonard Street: Duo Case Study," [Online]. Available: https://duo.com/use-cases/case-studies/stinson-leonard-street.

[62] "Two-Factor Authentication Using RADIUS," [Online]. Available: https://duo.com/docs/radius.

[63] Cyphercor, "2FA Case Study: LoginTC - Simple and Secure Two-Factor Authentication," [Online]. Available: https://www.logintc.com/case-studies/mdlive.html.

[64] Cyphercor, "Two factor authentication for RADIUS appliances," [Online]. Available: https://www.logintc.com/docs/connectors/radius.html.

[65] C. Inc, "Two factor authentication for RADIUS appliances," [Online]. Available: https://www.logintc.com/docs/connectors/radius.html#architecture.

[66] "Symantec™ VIP Intelligent Authentication [White Paper]," from SymantecVIP [Online]. Available:https://www.brendonwilson.com/wp-content/uploads/resume/samples/Symantec%20VIP%20Intelligent%20Authentication%20Technical%20Whitepaper.pdf.

[67] "Symantec™ VIP Intelligent Authentication Data Sheet," [Online].

Available: https://www-west.symantec.com/content/dam/symantec/docs/data-sheets/vip-intelligent-authentication-en.pdf.

[68] C. Mesa "Experian and Symantec Provide DrFirst with Identity Proofing and Authentication Technology," June 2011. [Online]. Available: https://drfirst.com/press-releases/experian-symantec-provide-drfirst-identity-proofing-authentication-technology/.

[69] "Symantec User Authentication Service Level Agreement [White Paper]," November 2014, from SymantecVIP [Online]. Available:https://www.websecurity.digicert.com/content/dam/websitesecurity/digitalassets/desktop/pdfs/repository/user-authentication-sla.pdf.

[70] "Self Service Portal considerations," [Online]. Available:https://help.symantec.com/cs/VIP_DEPLOY_GUIDE/VIP/v99477683_v126961060/Self-Service-Portal-considerations?locale=EN_US.

[71] "Duo Network Gateway," [Online]. Available: https://duo.com/docs/dng#web-application-diagram.

[72] "Duo Network Gateway," [Online]. Available: https://duo.com/docs/dng#ssh-servers-diagram.

[73] "Duo," [Online]. Available: https://duo.com/.

[74] "Tokens & Passcode," [Online]. Available: https://duo.com/product/multi-factor-authentication-mfa/authentication-methods/tokens-and-passcodes.

[75] "Duo generating Bypass code," [Online]. Available: https://duo.com/docs/administration-users#generating-a-bypass-code.

[76] "Multi-Factor Authentication from Duo," [Online]. Available: https://duo.com/product/multi-factor-authentication-mfa.

[77] "Duo Guide to Business Continuity Preparedness," [Online]. Available: https://duo.com/assets/pdf/Duo_Guide_to_Business_Continuity_Preparedness.pdf.

[78] "Duo Security and Reliability," [Online]. Available: https://duo.com/about/security-and-reliability.

[79] "Duo Pricing," [Online]. Available: https://duo.com/pricing.

[80] "Duo Service Level Agreement," 2018. [Online]. Available: https://duo.com/legal/sla.

[81] "Duo Overview," [Online]. Available: https://duo.com/docs/radius.

[82] "Duo Device Health Application," [Online]. Available: https://duo.com/docs/device-health.

[83] "Duo User Self-Service," [Online]. Available: https://duo.com/product/multi-factor-authentication-mfa/user-self-service.

[84] "Yubico Yubikey Products," [Online]. Available: https://www.yubico.com/products/.

[85] "Yubico Enterprise Solutions [White Paper] ,"from Yubico. [Online]. Available: https://cdn.brandfolder.io/53ZDUYE6/as/q5wwkk-3ldat4-ewrxma/Yubico_Enterprise_Solutions_Brief.pdf.

[86] "OTPs Explained," [Online]. Available: https://developers.yubico.com/OTP/OTPs_Explained.html.

[87] "Yubico Developer," [Online]. Available: https://developers.yubico.com/.

[88] "Yubico Open Source Server," [Online]. Available: https://www.yubico.com/products/services-software/open-source-servers/.

[89] "Yubico Services & Softwares," [Online]. Available: https://www.yubico.com/products/services-software/download/.

[90] "Yubico Remote Access & VPN," [Online]. Available: https://www.yubico.com/solutions/secure-remote-access-and-vpn/.

[91] "Yubico Warranty Information," [Online]. Available: https://support.yubico.com/support/solutions/articles/15000006431-yubikey-warranty-information.

[92] "Yubico OTP validation Server," [Online]. Available: https://developers.yubico.com/yubikey-val/.

[93] "Keeper business security," [Online]. Available: https://www.keepersecurity.com/pricing.html?t=b.

[94] "Enable secure priveleged access management," [Online]. Available: https://www.yubico.com/solutions/privileged-users/.

[95] "Yubico Support Services," [Online]. Available: https://www.yubico.com/support-services/.

[96] J. Chong "Yubico Expands FIPS Security Certification," March 2016 [Online]. Available: https://www.yubico.com/blog/yubikey-gains-support-for-higher-levels-of-federal-crypto-standards/.

[97] "Yubico Store," [Online]. Available: https://www.yubico.com/store/.

[98] " Losing Your YubiKey," November 2018. [Online].
Available: https://support.yubico.com/support/solutions/articles/15000006444-losing-your-yubikey.

[99] "SafeNet Authentication Service Service Provider Edition/Private Cloud Edition - subscription license (3 years) - 1 unit capacity," [Online]. Available: https://www.softchoice.com/catalog/en-us/applications-safenet-authentication-service-service-provider-editionprivate-cloud-edition-subscription-license-3-years-1-unit-capacity-Gemalto-VA8766.

[100] "Integration Guide. SafeNet Authentication Service. SAS Using RADIUS Protocol with NetMotion Mobility XE [White Paper]," August 2015, Document number:007-012561-001, from SafeNet [Online]. Available:https://docplayer.net/21198350-Integration-guide-safenet-authentication-service-sas-using-radius-protocol-with-netmotion-mobility-xe.html.

[101] "SAS Agent for Windows Logon 1.12 [White Paper]," June 2015, Document number:007-012394-002 from SafeNet [Online].Available:https://www2.gemalto.com/sas-downloads/docs/007-012394-002_SAS_Agent_for_Windows_Logon_1.12_Configuration_Guide_Rev_C.pdf.

[102] "SafeNet Authentication Service Push OTP Solution PDF [White Paper]," 2018, Document number:07-013306-00 from SafeNet [Online]. Available: https://safenet.gemalto.com/

[103] "SafeNet Authentication Service Proivder Administrator Guide PDF [White Paper]," March 2018, Document number: 007-012403-003 from SafeNet[Online]. Available:https://safenet.gemalto.com/

[104] "Safenet Authentication Service: Gemalto Authentication: Two Factor Authentication," October 2016. [Online]. Available: https://www.ecommnet.uk/it-security-solutions/two-factor-authentication/safenet-authentication-service/.

[105] "Offering affordable, Flexible, AutheNtications-A-Service," [Online].
Available: https://www.ecommnet.uk/wp-content/uploads/2015/05/SafeNet_Authentication_Service_Brochure.pdf.

[106] "SafeNet Authentication Client– Desktop Software for PKI-Based Authentication Management," [Online]. Available: https://safenet.gemalto.com/multi-factor-authentication/security-applications/authentication-client-token-management/.

[107] "SafeNet Technical Support," [Online]. Available: https://www3.safenet-inc.com/support/safeword/technical-support.aspx.

[108] Baltimore "SafeNet Authentication Service Achieves ISO 27001 Certification," February 2014 [Online]. Available: https://safenet.gemalto.com/news/2014/safenet-authentication-service-achieves-iso-27001-certification/.

[109] "SafeNet MobilePASS+ Push Authentication [White Paper]," from SafeNet [Online]. Available:https://safenet.gemalto.com/multi-factor-authentication/authenticators/software-authentication/mobilepass-plus-push-authentication/.

[110] "SafeNet Authentication Service - subscription license (1 year) - 1 user - 955-000001-001-003 - Authentication Software," [Online].Available:https://www.cdw.com/product/safenet-authentication-service-subscription-license-1-year-1-user/3960423#PO.

[111] "Sentinel Cloud Service Level Agreement [White Paper] ," from SafeNet [Online]. Available: https://sentinel.gemalto.com/Support_and_Downloads/Sentinel_Cloud_Service_Level_Agreement/.

[112] "Server Administration Guide [White Paper]," February 2019 from SecurEnvoy [Online]. Available: https://www.securenvoy.com/en-us/support#id3.

[113] "SecurAccess Benefits," [Online]. Available: https://www.securenvoy.com/en-us/SecurAccess/Benefits.

[114] "SecurEnvoy Launches New SecurAccess Virtual Security Appliance at Citrix Synergy," [Online]. Available: https://www.securenvoy.com/en-gb/blog/securenvoy-launches-new-securaccess-virtual-security-appliance-citrix-synergy.

[115] "SecurEnvoy Administration and Configuration Guide [White Paper]," February 2019. [Online]. Available: https://www.securenvoy.com/en-us/support#id3

[116] "Service Level Description,[White Paper]" [Online]. Available: https://www.securenvoy.com/en-gb/cloud-sla.

[117] R. Grimes, "11 ways to hack 2FA," May 2018. [Online]. Available: https://www.csoonline.com/article/3272425/11-ways-to-hack-2fa.html.

[118] K. Townsend, "NIST Denounces SMS 2FA - What are the Alternatives?," August 2016. [Online]. Available: https://www.securityweek.com/nist-denounces-sms-2fa-what-are-alternatives.

[119] K. Graham, "Identity 101: Why two-factor authentication is not enough," March 2018 [Online]. Available: https://www.ibtimes.co.uk/identity-101-why-two-factor-authentication-not-enough-1665422.

[120] "Going passwordless with Azure Active Directory," [Online]. Available: https://chrisonsecurity.net/2019/07/28/going-passwordless-with-azure-active-directory/.

[121] "Okta Passwordless Authentication," [Online]. Available: https://www.okta.com/passwordless-authentication/.

[122] "Passwordless Authentication," [Online]. Available: https://www.onelogin.com/learn/passwordless-authentication.

[123] "FIDO2: Moving the World Beyond Passwords using WebAuthn & CTAP," [Online]. Available: https://fidoalliance.org/fido2/.

[124] "Password-less Protection," [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2KEup.

[125] "Two-Factor Authentication Market by Type, Size, Growth and Forecast – 2024: MRFR," [Online]. Available: https://www.marketresearchfuture.com/reports/two-factor-authentication-market-3772.

[126] D. Storm, "9-vendor authentication roundup: The good, the bad and the ugly," June 2016. [Online]. Available: https://www.networkworld.com/article/3077843/9-vendor-authentication-roundup-the-good-the-bad-and-the-ugly.html.