Security and Performance of Knowledge-based User Authentication for Smart Devices

Alec Wells and Aminu Bello Usman
alec.wells@yorksj.ac.uk, a.usman@yorksj.ac.uk
Cyber Security Research Group
Department of Computer Science, York St John University, UK

ABSTRACT

A secure authentication system ensures that the claimant is the genuine user attempting to access the system and that it is not susceptible to misidentification, forgetfulness, or reproduction. While technological advancements in the authentication process continue to advance, most authentication systems still have room for improvement, particularly in terms of accuracy, tolerance to various security attacks, noise, and scalability as the number of smart devices grows. In this chapter, we look at the security, effectiveness, and drawbacks of knowledge-based, ownership-based, location-based, and social-based authentication systems, as well as some unresolved issues and potential future research directions.

Keywords: Secure Authentication System, Knowledge-based Authentication, Location-based Authentication, Ownership-based Authentication, Social-based Authentication, Smart devices.

1. INTRODUCTION

Authentication is the process of verifying an identity claim using the users' knowledge (e.g., secret questions, passwords, PINs), their possessions or ownership (e.g., ID cards, mobile phones, tokens), their location, other social accounts, or their biometrics (e.g., biometrics, fingerprints, iris scans, signatures) of which can all be referred to as different authentication factors (Flu, 2015). The purpose of authentication is to establish confidence, that the user trying to access technology, is the user themselves and to only allow the user access to their account/sensitive information. Strong authentication systems help to reduce potential fraudsters and other hackers from gaining access to sensitive information they should not have access to. The need of a secure authentication process is still a sizable concern in cyberspace to establish the integrity and authenticity of a claimant while accessing anything from technologies, applications to network systems. With the growth of smart technologies in many different sectors such as hospitals, financial sectors, the military, aviation, etc. there is an even greater need to determine the authenticity of a genuine user.

A secure authentication process ensures that the claimant is the legitimate user trying to access the system and the authentication process is not susceptible to misplacement, forgetfulness, or reproduction. Whilst technological progress in the authentication process continues to evolve, most of the authentication systems still have more room for improvement, particularly in their accuracy, tolerance to various security attacks, noisy environments, and scalability as the number of individuals increases (Poh, Bengio, & Korczak, 2002). The classification of user authentication factors can be seen in Figure 1, which classifies authentication factors in to five main categories, Knowledge-based, Biometric (inherence)-based, Ownership-based, Location-based, and Social-based authentication factors.

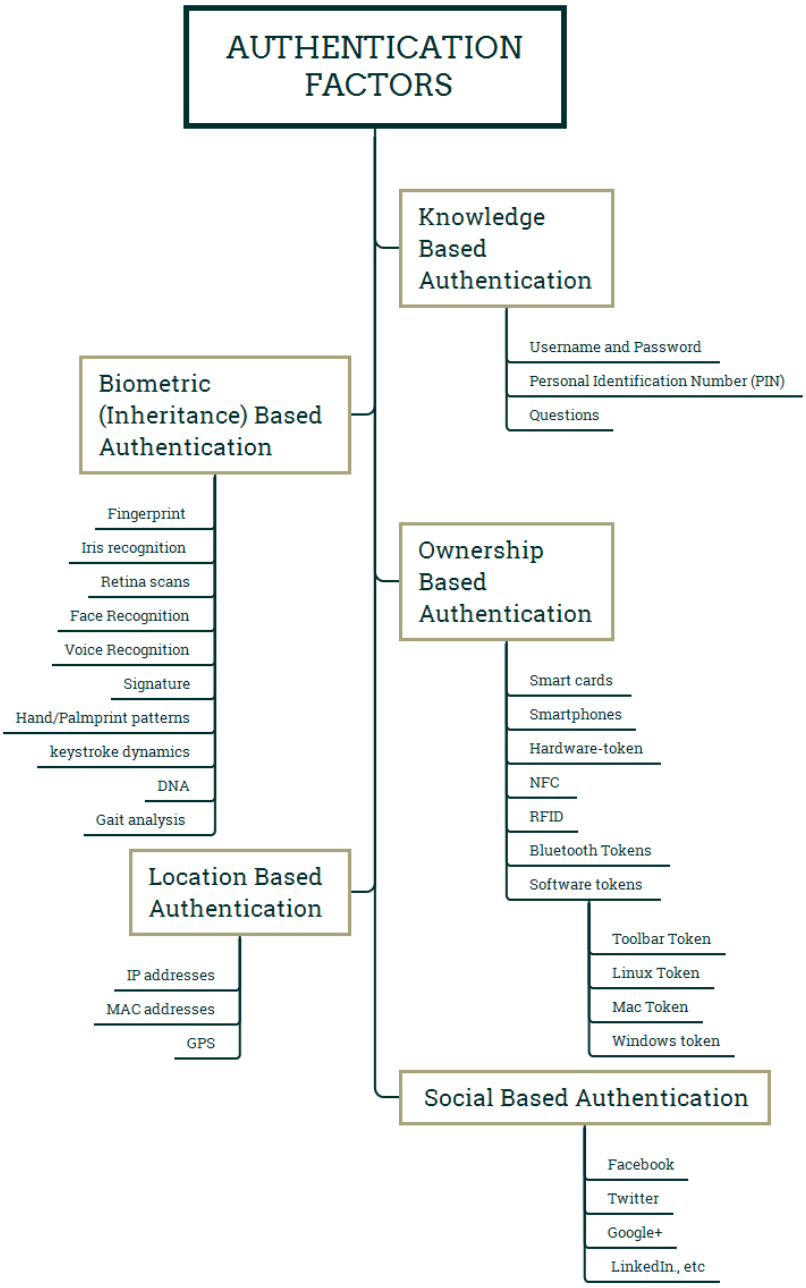

Figure 1. A Taxonomy of Authentication Factors - A breakdown of each authentication method and a list of examples for each type

The Knowledge Based Authentication (KBA) is a flexible tool in digital identity proofing protocols and solutions. As the name suggests, knowledge-based authentication factors seek to prove the identity of the claimant accessing the technology or service, using private and secret pieces of information to prove the claimant's identity. KBA can be offered in many formats, making it a valuable and flexible authentication mechanism in many cybersecurity architectures. Knowledge-based factors are based on information only the user should know such as a username and password or personal identification number (PIN).

Ownership-based authentication factors are based on something the user has, such as cards, smartphones, or other tokens. For instance, one of the most prevalent examples of ownership-based factors are payment cards, utilized by banks that each possess a unique combination of numbers and security information from one another. Another example of ownership-based factors is the usage of tokens that are issued to the user to use to sign in.

The location-based authentication factors use the claimant's identity to detect its presence at a distinct location (Trojahn & Marcus, 2012). It is based on the user being located within a certain vicinity in order to correctly authenticate them. This usually involves the user using a location-based client (LBC) to verify with a server

containing their location-based ID in order to authenticate themselves. Usually location-based authentication is used in combination with another form of authentication, however location-based authentication can also be used on its own, to get access to a machine or detecting that a person is at a specified area – such as an entrance.

The chapter is structured as follows: Section 2 presents an overview of authentication systems; specifically looking at the various different factors and how they are used in single and multi-factor authentication. Section 3 discusses knowledge-based authentication, again providing an overview and looking at the attacks done on KBA. Section 4 looks at ownership-based authentication comparing the types of token and also looking at the security issues of ownership-based authentication. Section 5 provides a brief look at location-based authentication and the challenges it presents. Section 6 discusses social-based authentication and its challenges. Finally, Section 7 is a conclusion of the findings within this study that also discusses open issues and potential future research.

The key research question of this chapter asks what is the current state of authentication methods as a whole? To answer this question, papers were researched between the time period of 1994-2020, using the following search terms: Authentication, Factor, Knowledge, Ownership, Token, Location, Attack, Brute-Force, Masquerade, Blended Substitution, False Acceptance, Phishing, Guessing, Password & Entropy. The search terms were used in databases IEEE, Science Direct, Springer and Google Scholar of which 87 articles are referenced.

2. AUTHENTICATION METHODS

Authentication methods can be categorized in two groups, single-factor authentication and multi-factor authentication. The descriptions of the two user authentication methods are provided in the following sections.

2.1 Single-Factor Authentication Methods

The single-factor authentication method simply involves using only one method or 'factor' to verify the user's identity and authenticate themselves. Single-factor authentication can involve any type of factor from knowledge-based factors like passwords or PIN numbers, to ownership-based factors such as bank cards or cell phones, other factors such as inherence factors like a user's fingerprints or iris, or social factors such as google accounts, or location factors such as their GPS location (Turner, 2016).

Many different literature, technology-based companies and agents consider single-factor authentication to be inadequate for preventing fraud, especially for that of high-risk transactions related to banking (Council, 2005) (Tiwari, Sanyal, Abraham, Knapskog, & Sanyal, 2011). This is simply because if you only have one factor protecting your account, if that was to ever leak, then access to the account can be immediately gained by an intruder. Studies such as (Vel´asquez, Caro, & Rodr´ıguez, 2018) also suggest that in regard to single-factor authentication using knowledge factors, users find it hard to remember passwords for a long time, or remember different passwords for multiple accounts, hence leakages are much more likely, without a second alternative factor also being used. This is especially a concern nowadays, considering the amount of data breaches that have occurred in recent years where multiple users accounts and passwords have been leaked. Even disregarding data breaches, many passwords can be cracked due to users using weak or even default passwords, allowing hackers easy access to accounts. When users are valuing authentication, the main considerations they have are with the usability and security of the authentication (Khan & Zahid, 2010). Although many users consider multi-factor authentication to be safer and more secure than single-factor, users also consider single-factor to be more user friendly, as shown in the study (Gunson, Marshall, Morton, & Jack, 2011) in which participants considered single factor to be easier, more straightforward and quicker than multi-factor authentication.

2.2 Multi-Factor Authentication Methods

Multi-factor authentication utilises a similar process to that of single-factor authentication. However, the primary difference between the two is that multi-factor authentication will only authenticate the user after they have presented two or more factors to verify their identity (Turner, 2016). Similar to single-factor authentication, these can be based on the same factors seen their such as knowledge, ownership, behavioral, location or social. In multi-factor authentication, the authentication process can ask for pieces of evidence from the same type of factor i.e. two knowledge-based factors like a password and security question or two different types of factor,

such as a fingerprint and PIN code.

Mutli-factor authentication while considered much more secure than single-factor authentication, does however have a few drawbacks. For instance, just like single-factor authentication, two-factor authentication is not immune to being hacked and is just as vulnerable to many different types of attacks. Another concern with multi-factor's feasibility is when only one factor is available to authentication themselves, such as for example, if a user is using a mobile authenticator, in a rare circumstance that mobile phone might not be available due to battery loss, lack of signal or it being stolen. Two-factor authentication can also be equally susceptible to users having their credentials stolen from phishing-based attacks. For instance, one such example is Man-in-the-Middle attacks, where attackers will create spoofed versions of websites for users to type their credentials into for the attacker to steal and use on the real website. Alternatively, other attacks that two-factor authentication is not immune to is the likes of Trojan attacks where a hacker can piggyback on a user's login session to make their own fraudulent transactions (Schneier, 2005).

The main deployment of multi-factor authentication has been through phone authentication apps that users can tie to most online accounts. This authentication follows the method of first receiving credentials that have one identifier between a first and second principal (such as an email address). The user's knowledge of the first identifier is first verified (such as a password) and an authentication credential is then generated (Burch & Carter, 2010). This is often seen with smartphones via an app to generate codes for the user to receive and then enter when they sign in (Drokov, Punskaya, & Tahar, 2015). This has been one of the most common deployments of multi-factor authentication due to how integrated phones are in modern society – allowing them to be nearly always available, except in extenuating circumstance.

Other prominent examples of multi-factor authentication are seen in the world of banking that utilizes both knowledge and possession-based factors. In order to pay via a credit card in person, a user must have both the bank card itself to put in the card reader and know the PIN code in order to complete the transaction. Alternatively, multi-factor authentication is seen for a network service by monitoring a session at a firewall applying a profile based on the new session and performing an action based on the authentication profile (Murthy, Ganesan, Mangam, Jandhyala, & Walter, 2020).

Overall, despite single-factor authentication being considered inadequate at preventing fraud, it is still commonly used as it considered both faster and more convenient for the user compared to the safer yet slightly more cumbersome multi-factor authentication. Several important services, such as banking, have multi-factor authentication as a requirement, whereas less important services simply provide it as an optional extra layer of security. Single-factor and multi-factor can be used with all different authentication factors in various combinations, such as with biometrics, when two different biometrics are combined together, is referred to as multimodal biometrics. This is elaborated in the following sections.

3. KNOWLEDGE-BASED AUTHENTICATION

The two most widely used methods of users' authentication using KBA are: static (shared secrets) and instant (also known as dynamic KBA). The Static KBA is based on a pre-defined or agreed set of questions or shared secret information between the authentication parties involved. Mostly, static KBA relies on factoid recall, which is information known specifically to the user, which include questions such as what your is mother's maiden name, what street did you grow up on, or what was your first pet etc, and is commonly used by email providers, banks, financial services or other companies to authenticate different users (Chokhani, 2004).

On the contrary, instant KBA uses methods and algorithms to dynamically develop a set of personal questions and answers to authenticate a user, and it does not require the user to have provided the questions and answers beforehand (Flu, 2015). These dynamic questions provide randomized right and wrong answer choices based on data found for the subject by the KBA system. Regardless, in practical usage, both versions of KBA usually require a form of initial registration against an existing database to create the credentials. KBA then usually requires access to the server to verify the factoids/credentials in the login mechanism (Chokhani, 2004).

One of the attributes of KBA is password entropy - a measure of how unpredictable a password is. Password entropy estimates how many trials an attacker (either by guessing or brute force) would need, on average, to guess the password correctly. In other words, the more difficult to predict or guess the password entropy, the more secure the KBA is. Given a password with a character size L, we can compute the password entropy using

the following equation 1 below (MLB9252, 2011).

$$E = Log_2(R^L) \quad (1)$$

Where E is the password entropy, R is the pool of unique password char- acters, and L is the number of characters in each password. Subsequently, R to the power of L is the number of possible password combination and the equation is the number of bits of entropy.

3.1 Security attacks on Knowledge-Based Authentication Factors

The KBA attacks Taxonomy in Figure 2 presents the classification of KBA attacks, of which there are a few main types we cover; social engineering, guessing attacks and brute force attack.

3.1.1 Social Engineering Attacks on Knowledge Based Authentication Factors

The social engineering (SE) attack is manipulating the target (a person) to obtain information by a social engineer – an attacker. So far, SE is the most superior form of KBA attacks as users themselves are the attacks' targets. Successful social engineering attacks can be incredibly damaging and highly lucrative. In a SE attack, the attacker takes on a legitimate personnel's disguise to convince the victim to give out their sensitive information. The attacker can execute the attack in person by interacting with the target to gather desired information about the target(s) or use specialized software. A distinctive feature of SE attacks to KBA compared with the other forms of attacks on KBA, is social engineering attacks exploits human weaknesses and that it may be challenging to address the problem of human weaknesses.

The attacks' operators of social engineering attacks against KBA can be classified into two approaches. Social engineering attacks include social-based attacks (using psychological skills to collect KBA information) (Granger, 2001) (Salahdine & Kaabouch, 2019), and computer-based attacks (the use of sophisticated technical tools to obtain KBA information) (Krombholz, Hobel, Huber, & Weippl, 2015). In turn, depending on how the attack is conducted, social engineering attacks can be classified into three categories, physical, technical and socio-technical (or social) based attacks. Physical-based attacks refer to physical actions the attack does, such as dumpster diving, to obtain information. Technical-based attacks refer to attacks using technical approaches – using technical tools and methods to harvest users' KBA information. Technical types of attacks to KBA are mainly carried out over the Internet using a specialized tool such as Maltego to gather and aggregate target's information from different Web resources or social networks. Finally, social-based attacks refer to exploiting relationships with the victim, utilizing psychology and emotion to trick the victim into giving information and is currently one of the most powerful forms of KBA attacks used by of social engineers. Examples of these forms of attacks include "road apples" attacks, an attack using a USB containing a Trojan horse or baiting attacks (Stasiukonis, 2006). Social-engineering attacks have often shown to be very effective, for example a study investigated the vulnerability of hospital employees sharing their passwords through social engineering attacks with 73% of respondents sharing their password (Medlin, Cazier, & Foulk, 2008).

Table 1 presents different forms of social engineering attacks in relation to two different approaches to social engineering attacks. Examples of attacks can include shoulder surfing attack, which is a form of social engineering attack used to obtain information from the target using direct observation techniques, such as looking over victim's shoulder to obtain victims' passwords, PINs, or secret information. Dumpster diving attack is another form of social-based attack to recover information about the habits, activities, and interactions of individuals or organization from discarded phone books, hard drives that have not properly been scrubbed or surfing through people's curbside garbage. "A dumpster can be a valuable source of information for attackers, who may find personal data about employees, manuals, memos and even print-outs of sensitive information" (Koyun & Janabi, 2017).

Attack Operator	Shoulder Surfing	Dumpster Diving attacks	Reverse Diving Attacks	Water holing attacks	Crawling or spidering attacks	Baiting Attacks	Advanced Persistent Threat	Spear Phishing attack	Voice Phishing Attacks	Man in the Middle Attacks	SMS Phishing	Catphishing	Clone Phishing	Whale Phishing
Social-Based Attack	✓	✓	✓		✓	✓		✓	✓			✓		
Computer-based Attack		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 1: Social Engineering Attacks' Operators on Knowledge Based Authentication Factors

The Reverse Social Engineering (RSE) attack has three stages: sabotage, advertising and assisting. Initially, an attacker can sabotage the company's or individual access credentials. The attacker can then convince the target that he/she is ready to solve the problem. "When the victim asks for help, the social engineer will resolve the problem they created earlier while, for example, asking the victim for their password ("so I can fix the problem") or telling them to install certain software, etc. (Krombholz et al., 2015)". Other forms of SE attacks on KBA include water holing attacks - strategically targeting frequent users of a website by infecting one or a few frequent users (Edwards, Larson, Green, Rashid, & Baron, 2017), spidering attacks - often a more automated and thorough form of phising attack gather all small details (Dale, 2021), baiting attacks - similar to phising attacks but as a Trojan horse, providing a good incentive or gift to the user in exchange (Fan, Lwakatare, & Rong, 2017), advanced persistent threat - which is repeated usage of the same technique to wear the victim down, often gaining and then maintain a foothold (Daly, 2009) and phishing attacks. We provide in the following section, a detailed description about phishing attack on KBA.

As presented in Figure 2 there are different forms of phishing attacks: whaling phishing, spear phishing attack, and vishing phishing, etc. Spear phishing attack is usually directed at specific individuals or companies to gather and use personal information about the target to increase chances of successful attacks (Ho, Sharma, Javed, Paxson, & Wagner, 2017). Whaling phishing (Whaling email) is a highly targeted phishing attack mostly against financial institutions and payment services. Through social engineering, the attacker can encourage the victim to perform a secondary action, such as initiating a wire transfer of funds. Whaling phishing are more sophisticated than generic phishing emails as they often target senior executives (Chiew, Yong, & Tan, 2018). Other forms of phishing attacks include the catfishing attack in which the attacker pretends to be someone else the target would be interested in, to lure the target into giving information they wouldn't usually give to the attacker (Simmons & Lee, 2020). There is also voice phishing and SMS phishing, which both involve the user spoofing phones either through landlines or SMS pretending to be someone else by changing their caller ID (Choi, lak Lee, & tae Chun, 2017) (Mishra & Soni, 2019). Clone phishing meanwhile is where an attacker takes something legitimate, such as a website or email and makes a copy of it, however, they can replaces attachments or links with something malicious or steal the users data (Banu & Banu, 2013). In the Man-in-the-Middle (MITM) phishing attack, the phisher places himself or herself in the middle of two ways communication between the victim and a web-based application to eavesdrop and collect sensitive information that the victim is submitting to a web-based application (Chiew et al., 2018).

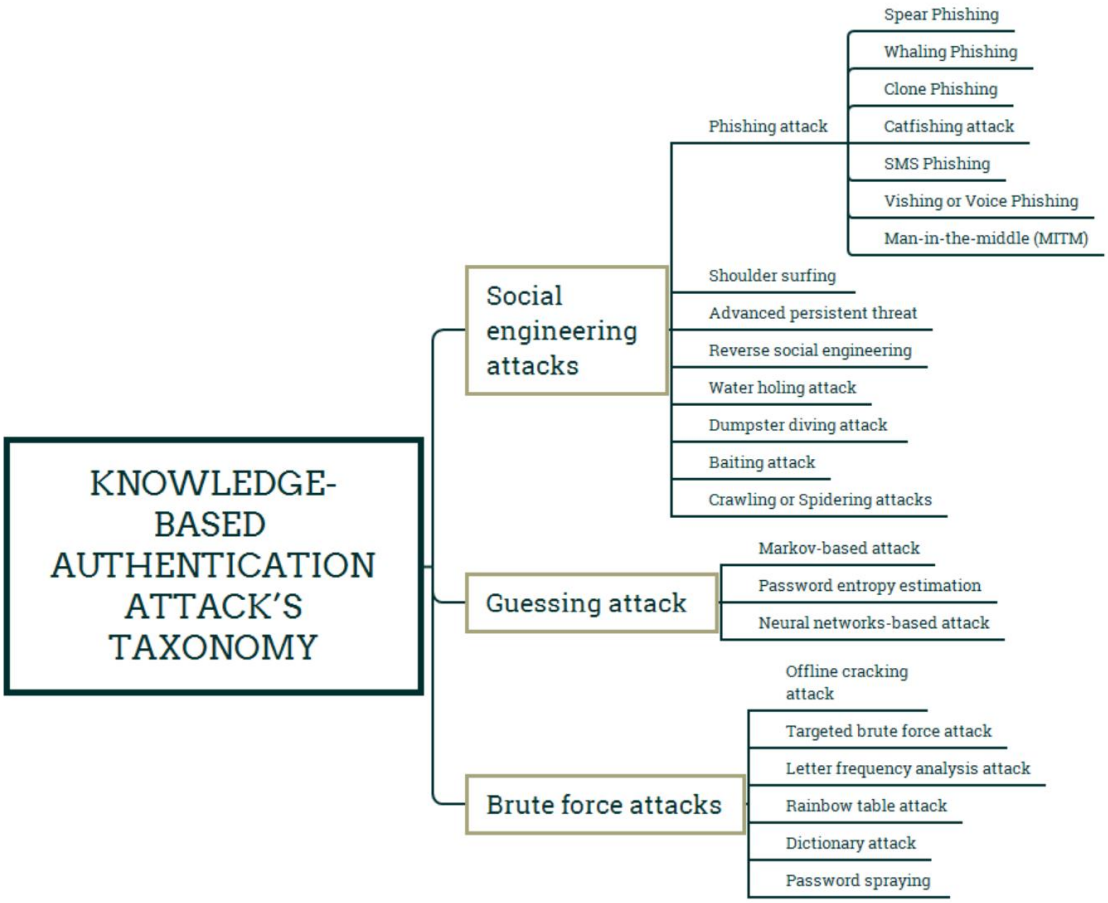

Figure 2: Knowledge-Based Authentication Attack's Taxonomy - An illustration of various types of knowledge-based authentication and the type of attacks they can be attacked by

3.1.2 Guessing attacks on Knowledge Based Authentication Factors

The popular methods of KBA guessing attacks can be classified into three types: Markov-based, neural networks-based (recognise relationships in data the same way a human brain operates), and Entropy estimation (guessing based on the expected entropy). The study (Narayanan & Shmatikov, 2005) argued that the distribution of letters in easy to remember KBA factors (e.g, passwords) is likely to be similar to the distribution of letters in the users' native language. The authors applied "Markov modelling techniques from natural language processing to reduce the size of the password space to be searched and increases the chances of guessing the password". Meanwhile the study (Durmuth, Angelstorf, Castelluccia, Perito, & Chaabane, 2015) proposed a "Markov model-based password cracker that generates password candidates according to their occurrence probabilities". The study (M. Weir, Aggarwal, Medeiros, & Glodek, 2009) applied a" probabilistic context free grammar based upon a training set of previously disclosed passwords template to generate word-mangling rules for password cracking". Finally, the study (Hitaj, Gasti, Ateniese, & Perez-Cruz, 2019) applied" machine learning algorithms to propose password guessing technique based on generative adversarial networks (GANs) to learn users' password distribution information from pass-
word leaks".

The use of Bayesian network (BN) models in probabilistic reasoning and information theory provide a valid metric for entropy estimation of human-selected passwords. The proposed BN-KBA model in (Y. Chen, 2007) is intuitively appealing in that it captures two key metrics of KBA as the model parameters, particularly the likelihood memorability (probability that a claimant with true identity recalls the factoid correctly) and guessability (the probability that an impostor correctly guesses the factoid). In that vein, the study (Y. Chen & Liginlal, 2007) proposed a methodology for implementing a Bayesian network based KBA system. The findings in the study suggested that in the context of KBA, the personal knowledge revealed from a variety of online sources can be directly or indirectly be exploited by imposters to attack a KBA system using the two metrics

(memorability and guessability). The other reason for KBA being compromised is due to the of predictability of user choice on the guessability of KBA. For example, given a password, the guessability of the password factoids can be computed using the following equation (Chokhani, 2004).

$$P_{KBA,j} = \pi_i P_{i,j}$$

Where P (KBA, j) is the probability of compromising KBA by j. The claimant type is j. The ith factoid factoid is i and the probability to guess by factoid i is Pi,j , subsequently, the convenience of a KBA system is valued as important as the obscurity (difficulty of guessing) variable; thus, guessability of KBA can be a reason why alternative solutions are being explored, though the guessability of KBA is made worse by the fact that many users use common, easy to guess passwords, such as '123456' which was used by over 23.2 million breached accounts (NCSC, 2019). In addition, with the rich data repository available on resources such as online social networks and the cutting-edge machine learning techniques, the guessability an attacker would achieve can be substantially improved. Subsequently resources such as online social networks, may put imprudent KBA designs at risk.

3.1.3 Brute Force attacks on Knowledge Based Authentication Factors

A brute force attack on KBA is the act of trial and error to gain access via trying multiple combinations of password. There are different forms of brute force attack to KBA including offline cracking attack (taking a password from a password storage file that has been recovered from the system) (Blocki, Harsha, & Zhou, 2018), letter frequency analysis attack (replace popular letters in ciphertext with common letters in the used language) (CRYPTO-IT, 2020), or targeted brute force attacks which primarily uses input dictionary creation programs and password guess generators (to target other accounts with previously compromised account details) (Tools, n.d.) (Salamatian, Huleihel, Beirami, Cohen, & M´edard, 2020). Another form of brute force attack on KBA is rainbow table attack which enables the recovery feasibility of long, human chosen passwords, which computes hashes of the large set of available strings, rather than specifically calculating a hash function for every string present and comparing them to the target (ParthDutt, n.d.) (Marforio, Masti, Soriente, Kostiainen, & Capkun, 2016) (L. Zhang, Tan, & Yu, 2017).

A more refined version of the brute force attack is a dictionary attack, a type of attack that only utilizes the possibilities most likely to succeed rather than cycling through every option like a brute force attack (Jablon, 1997). Similarly, password spraying also utilizes the most common passwords, but instead targets multiple accounts at once, to try to gain entry into any account regardless of the user (Joseph, Bruchim, Gofman, & Ashkenazy, 2021). There also exists the danger of password cracking, where attackers try recover passwords from data that has already been transmitted, usually via a brute-force attack, however since the password has already been transmitted the attackers know the cryptographic hash of the password, allowing them to brute-force more effectively (C. M. Weir, 2010).

While there are many different attacks against knowledge-based factors, there are several countermeasures that users can do, to try make them as secure as possible. One of the simplest and yet best ways to deal with various attacks, is to have strong, uncommon passwords that utilize multiple different types of characters, numbers, and case (Shay et al., 2014). By using stronger passwords, simple attacks such as brute-force and dictionary attacks are far less likely to succeed. Likewise, having different passwords for every account or changing passwords often can help keep accounts secure in the event of a data breach, though many would argue that" changing password often can inflict needless pain, cost and risk to the user," (Lance, 2019) though could still be considered good practice. Beyond that, users should simply be careful to avoid any suspicious software/emails and always look for good identifiers, such as the padlock in the address bar to signify the website is encrypted. Depending on the types of attacks, other forms of attacks' countermeasures include multi-factor authentication, account lockouts after multiple failed attempts, user training, and antivirus software (Dejan, 2018). Alternatively, the study (Bhardwaj & Goundar 2021) proposes for preventing brute force attacks on Cloud services that a 3 tier structure is superiors to that of single tier infrastructure, applying various firewalls to different tiers such as networks and web applications.

Despite the perceived risk of KBA, it is still widely used and has many metrics." KBA is very easy to use and easy to understand. This is because it has been one of the standard means of authentication and KBA, such as

passwords, are the most common form of authentication" (for Cybersecurity, n.d.). Likewise, from an admin and logistical point of view, KBA is very attractive. It requires no additional hardware beyond a standard keyboard, unlike for instance biometrics, which means it can be easily used by anyone for anything and anywhere. Due to this, it is cheaper to implement for business than more costly methods, such as biometrics (Raza, Iqbal, Sharif, & Haider, 2012), and is also fairly easy to administer for both home and business owners. Further, studies have suggested that the possible starting point for addressing the vulnerability of KBA credentials is to understand the status of uses' password reuse behavior since many studies suggested that the same login credentials are used for many more accounts and reused much more often than previously expected (Bang, Lee, Bae, & Ahn, 2012).

4 OWNERSHIP-BASED AUTHENTICATION

Ownership-based authentication factors are based on something the user has, such as cards, smartphones, tokens etc. For instance, one of the most prevalent examples of ownership-based factors are payment cards, utilized by banks that each possess a unique combination of numbers and security information from one another. Another example of ownership-based factors is the usage of tokens that are issued to the user to use to sign in. As we've moved into a more digital age, one of the most common forms of ownership-based factors is within mobile phones to deliver a single use code, either through receiving a code through text messages or via an authentication-based app that would provide a code when you attempt to login.

Payment cards are an extremely common form of ownership-based factors and are usually issued by banks. A bank card has a unique string of numbers as well as data such as an expiry date and security code that is tied to a user's band account. Bank cards can come in many different forms, with the most common being credit and debit cards. Similarly, many banks also use a form of tokens (electronic key) or one-time use passwords (a password that is generated for that specific sign-in request) to authenticate users and the server. Authentication apps and messages are being used for a variety of online accounts to be used in conjunction with passwords as a form of two-factor authentication, some examples include the google authenticator and windows authenticator apps. Alternatively, mobile phones can also be used as a token by using Bluetooth wireless communication, using the phone token as a challenge-response protocol (Kunyu, Jiande, & Jing, 2009). We also see tokens being applied to cloud computing, as seen when multi-layer tokens were used with honey passwords to authenticate users at different fog nodes to deter various attacks such as should surfing, password guessing and denial of service attacks (Rayani, Bhushan, & Thakare, 2018). Another form of ownership-based authentication is a smart card or integrated circuit card (ICC card) - an electronic authorization device, used to control access to a resource. The ICC card is typically a plastic credit card-sized card with an embedded integrated circuit (IC) chip (ISO/IEC, 2007). A smart card can be in either the form of card with metal contacts to electrically connect to the internal chip, connect contactless, or in both forms (Kuo & Lo, 1999). Smart cards contain a users' authentication, small data storage, and application processing components to perform input/output (I/O) functions. In terms of applications, most organizations used smart cards for single sign-on (SSO) (using the same ID for multiple services) for pass-through authentication system. For example, studies such as (X. Li, Xiong, Ma, & Wang, 2012) and (X. Li, Niu, Khan, & Liao, 2013) have proposed schemes that utilized smart cards for scenarios such as multi-server architecture and insecure network environments. Both approaches include a control server which chooses a master key and four phases: registration, login, authentication/session key and the password change phase. Alternatively, the study (C.-T. Li & Hwang, 2010) also proposed a smart card scheme that uses a one-way hash function with verification and smart cards that is unique due to the usage of randomized numbers in place of timestamps for resisting replay attacks. Another example is in the study (X. Li, Niu, Ma, Wang, & Liu, 2011), which proposed a improved biometric scheme using smart cards that supports session key agreements, which allowed the scheme to be more resistant to man-in-the-middle attacks. Other forms of ownership-based factors include NFC (near-field communication)-tag authentication, which uses a unique key that is encoded onto the tag, which when scanned reveals the item (W.-D. Chen, Hancke, Mayes, Lien, & Chiu, 2010). RFID (radio frequency identification) involves a similar process to NFC- tags but transmits the data using radio waves (Lim & Kwon, 2006). Cellphones can be used as ownership-based factors in many ways from providing one-time passwords through phone apps and SMS messages or as digital certifications using public key infrastructure (Contributor, 2014). Finally, hardware-tokens, which come in several forms, which we expand upon in the following section (Shablygin, Zakharov, Bolotov, & Scace, 2013).

4.1 Categories of Hardware-Token

Hardware-token can be categorized into synchronous and asynchronous Tokens. For synchronous tokens, time

synchronization between the token and authentication server is used as part of the authentication process, whereas asynchronous does not.

4.1.1 Synchronous Tokens

With synchronous token, a server keeps the records of a serial number for each authorized token, the user associated with the token, and the time. Using these three pieces of information, a server can predict the dynamic code generated by the token. As illustrated in Figure 3, synchronous tokens have two subcategories of which they can be, either clock-based or counter-based tokens. The clock-based, One Time Password (OTP) tokens are dependent on time-sensitive codes which have to be used within a certain timeframe, often expiring if not used within the correct amount of time. Many authentication apps are time based and will have to be used quickly before being replaced by another key. This means usually only the user will have enough time to access the correct code within the necessary time window (Jøsang, 2018).

The second type of synchronized token is counter-based OTP tokens. Counter-based OTP tokens (sometimes referred to as event-based OTP) generate a form of 'password' from two pieces of internal information. The two pieces of information are the secret key (or seed) which is only known by the token and the second piece of information is the moving factor, aka the counter. To give out a token, the OTP feeds the counter number into an algorithm with the token seed as the key; this produces a 160-bit value that is reduced down usually to 6-8 digits for the user to use as an OTP. When the token is pressed, the counter is incremented when a OTP is successfully validated. The key difference between counter and clock-based OTP is that counter-based uses purely internal data rather than external data (Smith, 2018).

4.1.2 Asynchronous Tokens

Alternative to synchronised tokens are asynchronous tokens, also known as challenge-response tokens. Challenge-response authentication defines one party proposes a challenge or question to the other. The second party can then perform the challenge or task by using information only available to it. The types of challenge questions can be static or dynamic. Static questions are predefined that the user has previously selected for instance "name of first pet" etc. Dynamic questions are created from extracting public data about the user such as a "previous street address" (Jøsang, 2018) (Rouse, 2018). Asynchronous tokens are not synchronized with a central server" and thus, the most common types are challenge-response tokens. Challenge-response authentication is often done using cryptographic techniques to prevent eavesdropping. Hence, many challenge-response tokens use encryption keys when generating the challenge, so that the responder must also use the key to create an encrypted response (Konigs, 1991).

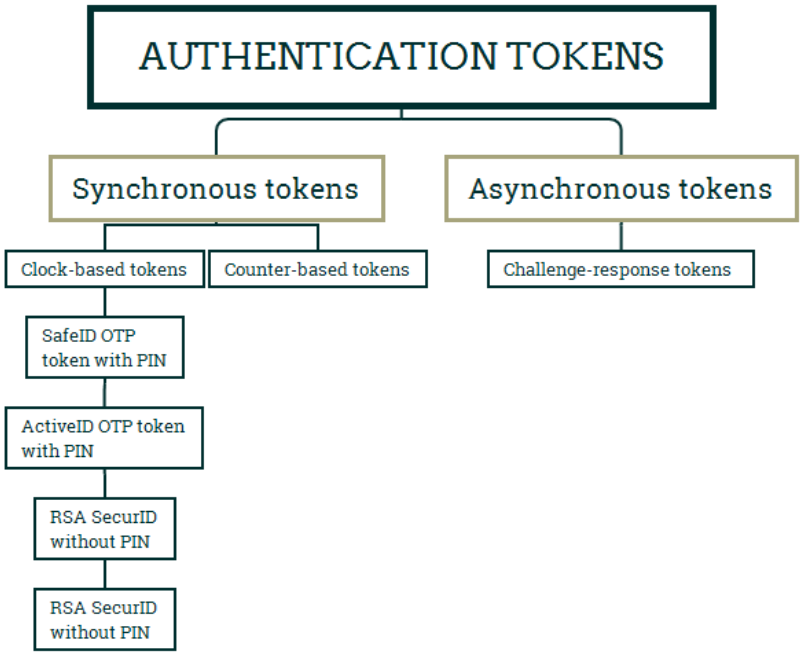

Figure 3. Categories of Authentication Tokens - A breakdown of the two types of tokens and various examples of each

4.2 Client to Authenticator Protocol

Alternatively, other types of ownership authentication exist. For example, with smartphones, protocols such as FIDO2, which is a form of password less authentication that uses WebAuthn and the FIDO Client to Authenticator Protocol 2. FIDO2 is able to authenticate the user by contacting a device such as a mobile phone, this could be done via the use of biometric features, such as by using touch ID. FIDO2 then uses a challenge-response protocol by using a pair of keys, that are individually generated for each service, that when verified, will authenticate the user (Lyastani, Schilling, Neumayr, Backes, & Bugiel, 2020). This approach is different in that it doesn't use tokens and hence is not susceptible to the likes of phishing or credential stuffing attacks since no text message or token is inputted by the user. FIDO2 improves upon the base of the original FIDO which only covered using public key cryptography for mobile devices, whereas FIDO2 also supports browsers from Microsoft, Mozilla and Google and is being adopted by many areas such as banking, telecoms and other sectors (Dunkelberger, 2018).

Many believe that passwordless authentication can be the future of authentication, due to it lacking the use of passwords, which is important as 81% of data breaches are caused by stolen or weak passwords (Enterprise, 2017) and nine out of ten phishing attacks target the users' credentials such as passwords (Enterprise, 2016). However, passwordless authentication is still relatively new and studies have sought to investigate user opinions with passwordless authentication as single factor authentication to determine if users are willing to accept a replacement for passwords (Lyastani et al., 2020).

4.3 Security Issues of Ownership-Based Factors

Ownership-based factors, however, are not immune to being hacked and they too have disadvantages that can inconvenience the user. The simplest problem with ownership-based factors is in the event that the user loses possession of their factor, or worse it is stolen, then the user cannot access their account and the user would both require a replacement token and request for the old card/token to be made invalid. When the data of an ownership-based factor is fixed, like for banking cards such as debit and credit cards, the individual details on them are at risk of phishing-based attacks and due to the rise of online commerce and banking, has made these details more vulnerable to those types of attacks. In 2016, 1.09 million banking Trojan attacks were detected and 47.78 percent of them were from the usage of a phony banking website/page to steal credentials from users (Stephen, 2019). Most phishing attacks are due the naivety of many users in signs of phishing and hence being unable to distinguish real sites from fake sites. Studies have looked into protocols that leverage communication between the service to provide security alert indications when in the presence of malicious applications for mobile devices, though even these require the user to be careful and alert for potential phishing (Marforio et al., 2016).

There are studies in the literature that have found that utilizing text message-based authentication can also be insecure, when researchers were able to get into a Gmail account to hack Gmail, all they required was a name and a phone number. The hackers were able to exploit a SS7 weakness to intercept SMS text messages from only knowing the number itself, allowing them access into Gmail accounts through password resetting and then proceed to do another reset (Thomas, 2017). This shows the dangers of having multi-factor authentication can also add more vulnerabilities to security, as hackers could be intercepting the codes, despite the user having possession of the device. Tokens have many vulnerabilities, though given there are many different types of tokens, these are not mutually exclusive. Tokens share the most common issue with ownership-based factors being the user either losing it, or having it stolen. In the event of having a card/token stolen, a user could be compromised, which is why tokens and other ownership-based factors are usually used in conjunction with knowledge-based factors as multi-factor authentication. However, credit cards are also vulnerable to SQL injection attacks as well as unpatched systems, or storage of unnecessary data (Braintree, 2007). In addition, systems utilizing a network for authentication can be vulnerable to man-in-the-middle attacks, where the attacker spoofs the" go-between" to solicit the token output from the user. Alternatively, a compromised token may be used for an SQL injection attack (maliciously entering an SQL statement into an entry field to be executed by the system) to tamper with the database containing user's data by exploiting input validation flaws.

5 LOCATION-BASED AUTHENTICATION

Location-based authentication (LBA) factors are more uncommon compared to the likes of knowledge or ownership-based factors. LBA is based on the user (or an object) being located within a certain vicinity in order to correctly authenticate them. This usually involves the user using a location-based client (LBC) to verify with a server containing their location-based ID to authenticate themselves or alternatively perhaps a consumer might

use a portable consumer device that is used to conduct a transaction at a merchant (F. Zhang, Kondoro, & Muftic, 2012). Mostly, LBA is used by financial industries to increase profitability of credit card companies by reducing the accumulated losses due to fraud.

Technology companies and network administrators are using building services that use geolocation security checks to verify the location of a user before granting access to an application, a network or entire system, like for instance GPS. For example, network administrators are using IP addresses to access the origin of network traffic and to know ascertain the users' location before granting service to the user. However, this can be bypassed by using IP tunneling (a channel between two networks to transport a network protocol) (Koutny & Sykora, 2010), a VPN or anonymous routing protocols (a specific way routers communicate with one another) (Kumari & Kannammal, 2009). In addition, MAC addresses, which are unique to individual computing devices, can be implemented as a location-based authentication factor to ensure that a system is only accessed from a limited number of authorized devices (Turnbull & Gedge, 2012). Location-based authentication can also be used to discern that a user has perhaps been compromised, as for instance it would seem odd a user that usually logs in within a certain postcode would be logging in from a different machine perhaps located on the other side of the world.

Location-based authentication systems with mobile devices transitions, is mostly used for electronic transactions on a financial institution's online website. The process of authentication may involve verifying whether a mobile device (such as a cellular telephone) is proximate to a computer from which the transaction is being performed (Ashfield, Shroyer, & Brown, 2012). If the mobile device is sufficiently proximate, then the transaction may be approved. Otherwise it can be rejected. To enable location-based authentication, a special combination of objects is required. First, the claimant must present a sign of identity. Secondly, the individual who is to be authenticated has to carry at least one human authentication factor that may be recognized on the distinct location and thirdly, the distinct location must be equipped with a means capable to determine the coincidence of individual at this distinct location (Hammad & Faith, 2017). Some studies investigated different forms of location-based authentication in a product supply chain with machine-learning techniques, by which they show suspicious products can be automatically recognized from the incomplete location information (Lehtonen, Michahelles, & Fleisch, 2007). To detect fraudulent transactions, studies have proposed a Location-based Authentication (LBA) system by which a fraud-score can be generated to indicate whether an attempted transaction should be authorized or not. (Eden & Avigad, 2012).

5.1 Challenges of Location-Based Authentication

Location-based authentication is not without its issues however, for instance one large consideration about location-based authentication is that the location used by a user is more publicly available knowledge than that of a password. Attackers could learn of a user's location through various tracking means and then appear at that same location. The accuracy of GPS signals is also crucial to the success of location-based authentication (Sharma, 2005). Alternatively, more sophisticated hackers might be able to spoof their location through various means such as through a VPN meaning that the location-based authentication would have to be more sophisticated to prevent this (Harber, 2022). Location-based authentication also relies on generating cryptographic keys based on the user's location which in turn could be brute-forced by an attacker, especially if that attacker knew the rough location of a user which would reduce the amount of attempts for a brute-force attack dramatically.

Location-based authentication does however have many advantages. Primarily adding an extra layer to authentication as it will only allow successful sign in from specific locations. This could be useful for a company that would only want employees on site being able to login, or for regular users with their home desktops only allowing specific locations such as their house or on mobile the town/city they live in. Unlike ownership-based factors, location-based factors cannot be stolen. Also, if location-based factors were being used for a certain building or home, then unlike most other authentication factors there could be several physical layers of protection, primarily door locks etc. to keep unwanted hackers from getting in. It also isn't necessary to set up specialized infrastructure for location-based authentication as it can be built into existing devices and mobile networks (F. Zhang et al., 2012).

6 SOCIAL-BASED AUTHENTICATION

Throughout the last few years, many web-based logins have adopted the ability to use social login. Social login allows users to authenticate themselves for services by using a login from their preferred social network account

such as Facebook, Twitter, Google, LinkedIn and many others, rather than setup an account with the service. There are many benefits to using a social login instead of having an account for each online service. For example, users don't need to remember multiple usernames and passwords for their accounts, the user establishes one connection to a reliable identity provider, which provides "reduced password fatigue" and lowers the need for the website to have significant infrastructure or security protocols" (Gafni & Nissim, 2014). Similarly, certain social media accounts are also being used for single sign on, such as Facebook, which allows users to use a single set of login credentials to access multiple services. In turn, by using single sign-on, it helps uses mitigates the need to manage and remember their different accounts and passwords (Fang, Kao, Milman, & Wilson, 2001).

6.1 Challenges of Social-Based Authentication

Social login however does have some concerns. For example, one issue is the privacy of the user. Many sites ask the user for lots of unnecessary personal information, not to mention any account would in turn be linked to the user's social media, which means users may lack anonymity on certain websites. This is also concerning as those websites with less infrastructure and security could be more easily compromised. A concern many users may have when using social login, is that if an attacker were to gain access to the user's social media, then they would potentially be able to access many accounts through their social login, hence strong passwords are a must (Gafni & Nissim, 2014). By using services for social-based or single-sign on, users are also creating a single point of failure so that if that service was ever down, they would be unable to access any of their other services, making them especially vulnerable to denial-of service attacks (Ellison, Hodges, & Landau, 2002).

7 CONCLUSION

In conclusion, many traditional means of authentication are considered to be outdated. Hence, many alternate methods of authentication are being sought out. Example of such outdated methods include; knowledge-based factors like passwords which while considered the norm and are widely used - have many potential security concerns as identified in section 4. This includes social-based attacks and computer-based attacks like social engineering, brute force and guessing-based attacks. As outlined in section 5, ownership-based authentication similarly has concerns being used as the sole means of authentication due to concerns such as misplacing or having the authentication factor being stolen, hence can only really be used in multi-factor-based authentication. Likewise, location-based authentication as presented in section 6 also displays many challenges, such as technologies like a VPN that can spoof sensors, as well as in section 7 in which presents the issues with social-based authentication mainly that it creates a single point of failure.

7.1 Open Issues

There are many open challenges that need to be solved in the field of authentication, such as the user's opinion and usage of knowledge-based factors. Given that they are the standard mode of authentication yet are often considered one of the weaker authentication factors. Hence there is a general need for better cyber hygiene amongst users, given the user themselves is often considered the factor most likely to cause a security breach, there needs to be a better way of keeping the user safe. For ownership-based authentication, although it can be attacked like other forms of authentication, one of the standout challenges currently is SQL injection attacks, being very popular for hacking common ownership factors such as credit cards, as hackers can gain the access to the details of the item, without owning the item. One topic of research interest would be developing better protection from SQL injection attacks for ownership-based factors. Specifically, regarding location-based authentication; one of the biggest open issues facing location-based authentication is the use of VPNs or Virtual Private Networks which are becoming increasingly popular. The reason is because with a VPN, a user could mask their position from where they are logging in from, disrupting the accuracy of the location-based authentication, hence, it could be important to solve this issue in the coming future. One issue that plagues all authentication types is the concern for privacy, which has come to the forefront after the introduction for GDPR regulations. As such many authentication methods should better consider how they will handle users' data in order to keep the users' data safe and private.

7.2 Future Research

Cloud computing and multi-server networks has had a large spike in activity over the last few years with many services offering more ways to utilize cloud computing or virtual desktop devices, though with new technology there are also new vulnerabilities and it is important to develop sufficient countermeasures and understand the possible dangers of using technologies to be prepared against them. Alternatively, there are many promising developments with virtual reality, with many considering it as a possible means of authentication. Studies could

investigate users' opinions on using virtual reality as a means to authentication themselves or how virtual reality is able to handle different attacks. To a lesser degree there is a similar interest in developing augmented reality technologies and similarly to virtual reality, may be considered as a possible means of authentication and how to best authenticate oneself while using augmented reality. Such research topics could be investigating users' opinions of authentication or investigating the attacks on augmented reality and defenses. Given all forms of authentication suffer from privacy concerns after the introduction of GDPR regulations it is of importance that privacy is considered in the design of authentication systems. Once such future research to address these could be the implantation of privacy principles such as privacy by design when designing privacy concerning authentication solutions, for example a framework of authentication.

REFERENCES

Ashfield, J., Shroyer, D., & Brown, D. (2012, October 23). Location based authentication of mobile device transactions. Google Patents. (US Patent 8,295,898)

Bang, Y., Lee, D.-J., Bae, Y.-S., & Ahn, J.-H. (2012). Improving information security management: An analysis of id–password usage and a new login vulnerability measure. international journal of information management, 32 (5), 409–418.

Banu, M. N., & Banu, S. M. (2013). A comprehensive study of phishing attacks. International Journal of Computer Science and Information Technologies, 4 (6), 783–786.

Bhardwaj, A., & Goundar, S. (2021). Comparing single tier and three tier infrastructure designs against DDoS attacks. In Research Anthology on Combating Denial-of-Service Attacks (pp. 541-558). IGI Global.

Blocki, J., Harsha, B., & Zhou, S. (2018). On the economics of offline password cracking. In 2018 ieee symposium on security and privacy (sp) (p. 853-871). IEEE.

Braintree. (2007, November 29.). Top 5 vulnerabilities leading to credit card data breaches (Vol. 2020) (No. 01/09/). Retrieved from https://www.braintreepayments.com/blog/top-5-vulnerabilities-leading-to-credit-card-data-breaches/

Burch, L. L., & Carter, S. R. (2010, June 15). Methods and systems for multi- factor authentication. Google Patents. (US Patent 7,739,744)

Chen, W.-D., Hancke, G. P., Mayes, K. E., Lien, Y., & Chiu, J. H. (2010). Using 3g network components to enable nfc mobile transactions and authentication. In 2010 ieee international conference on progress in informatics and computing (Vol. 1, p. 441-448). IEEE.

Chen, Y. (2007). A bayesian network model of knowledge-based authentication. AMCIS 2007 Proceedings, 423.

Chen, Y., & Liginlal, D. (2007). Bayesian networks for knowledge-based authentication. IEEE Transactions on Knowledge and Data Engineering, 19 (5), 695-710.

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications, 106 , 1-20.

Choi, K., lak Lee, J., & tae Chun, Y. (2017). Voice phishing fraud and its modus operandi. Security Journal , 30 (2), 454-466.

Chokhani, S. (2004). Knowledge based authentication (kba) metrics. In Kba symposium-knowledge based authentication: Is it quantifiable.

Contributor, T. T. (2014, December). What is mobile authentication? (Vol. 2022) (No. 02/02/). Retrieved from https://www.techtarget.com/searchsecurity/definition/mobile-authentication

Council, F. F. I. E. (2005). Authentication in an internet banking environment. FFIEC gencies (August 2001 Guidance).

CRYPTO-IT. (2020, -03-09). Frequency analysis (Vol. 2020) (No. 29th June). Retrieved from http://www.crypto-it.net/eng/attacks/frequency-analysis.html#:~:text=Frequency%20analysis%20is%20one%20of,are%20used%20with%20different%20frequencies.&text=Based%20on%20that%2C%20one%20can,texts%20written%20in%20other%20languages

Dale, W. (2021, 7 Sep). The top 12 password-cracking techniques used by hackers (Vol. 2022) (No. 02/02/). Retrieved from https://www.itpro.co.uk/security/34616/the-top-password-cracking-techniques-used-by-hackers

Daly, M. K. (2009). Advanced persistent threat. Usenix, Nov , 4 (4), 2013–2016.

Dejan, T. (2018, December 3,). How to prevent brute force attacks with 8 easy tactics (Vol. 2022) (No. 02/02/). Retrieved from https://phoenixnap.com/kb/prevent-brute-force-attacks

Drokov, I., Punskaya, E., & Tahar, E. (2015, January 27). System and method for dynamic multifactor authentication. Google Patents. (US Patent 8,943,548)

Dunkelberger, P. (2018). Fido2 puts biometrics at heart of web security. Biometric Technology Today, 2018 (8), 8–10.

D¨urmuth, M., Angelstorf, F., Castelluccia, C., Perito, D., & Chaabane, A. (2015). Omen: Faster password guessing using an ordered markov enumerator. In International symposium on engineering secure software and systems (p. 119-132). Springer.

Eden, T., & Avigad, B. (2012). Location based authentication system. (US Patent US8321913B2)

Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. Computers & Security, 69 , 18-34.

Ellison, G., Hodges, J., & Landau, S. (2002). Security and privacy concerns of internet single sign-on. Liberty v1 , 6 (2002.12).

Enterprise, V. (2016). Data breach investigations report. Report, Verizon Enterprise.

Enterprise, V. (2017). 2017 data breach investigations report.

Fan, W., Lwakatare, K., & Rong, R. (2017). Social engineering: Ie based model of human weakness for attack and defense investigations. International Journal of Computer Network & Information Security, 9 (1).

Fang, Y., Kao, I.-L., Milman, I. M., & Wilson, G. C. (2001, June 5). Single sign-on (sso) mechanism personal key manager. Google Patents. (US Patent 6,243,816)

Flu, K. (2015, TUESDAY, JUNE 2,). Knowledge-based authentication (kba). for Cybersecurity, E. U. A. (n.d.). Authentication methods (Vol. 2020) (No. 18/06/). Retrieved from https://www.hsgac.senate.gov/imo/media/doc/Testimony-Fu-2015-06-02-REVISED%2021.pdf

Gafni, R., & Nissim, D. (2014). To social login or not login? exploring factors affecting the decision. Issues in Informing Science and Information Technology, 11 (1), 57–72.

Granger, S. (2001). Social engineering fundamentals, part i: hacker tactics.
Security Focus, December , 18 .

Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-

factor and two-factor authentication in automated telephone banking. Computers & Security, 30 (4), 208-220.

Hammad, A., & Faith, P. (2017). Location based authentication. (US Patent US10163100B2)

Harber, L. M. (2022, January 19th). Fake gps: top 5 vpns for spoofing your location (Vol. 2022) (No. 02/02/). Retrieved from https://www.tomsguide.com/uk/best-picks/fake-gps-vpn

Hitaj, B., Gasti, P., Ateniese, G., & Perez-Cruz, F. (2019). Passgan: A deep learning approach for password guessing. In International conference on applied cryptography and network security (p. 217-237). Springer.

Ho, G., Sharma, A., Javed, M., Paxson, V., & Wagner, D. (2017). Detecting credential spearphishing in enterprise settings. In 26th USENIX security symposium (USENIX security 17) (p. 469-485).

ISO/IEC. (2007, -10). Identification cards — integrated circuit cards — part 2: Cards with contacts — dimensions and location of the contacts. (2).

Jablon, D. P. (1997). Extended password key exchange protocols immune to dictionary attack. In Proceedings of ieee 6th workshop on enabling technologies: Infrastructure for collaborative enterprises (p. 248-255). IEEE.

Joseph, T., Bruchim, G. Z., Gofman, I., & Ashkenazy, I. G. (2021, August 31). Credential spray attack detection. Google Patents. (US Patent 11,108,818)

Jøsang, A. (2018, Autumn). Lecture 9: User authentication (Vol. 2020) (No. 29th June). Retrieved from https://www.uio.no/studier/emner/matnat/ifi/IN2120/h18/lectures/in2120-2018-l09-user-authentication.pdf

Khan, H. Z. U., & Zahid, H. (2010). Comparative study of authentication techniques. International Journal of Video & Image Processing and Network Security IJVIPNS , 10 (04), 9.

Konigs, H.-P. (1991). Cryptographic identification methods for smart cards in the process of standardization. IEEE Communications Magazine, 29 (6), 42–48.

Koutny, T., & Sykora, J. (2010). Lessons learned on enhancing performance of networking applications by ip tunneling through active networks. International Journal on Advances in Internet Technology Volume 3, Number 3 & 4, 2010 .

Koyun, A., & Janabi, E. A. (2017). Social engineering attacks. Journal of Multidisciplinary Engineering Science and Technology (JMEST), 4 (6), 7533-7538.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22 , 113-122.

Kumari, E. H. J., & Kannammal, A. (2009). Privacy and security on anonymous routing protocols in manet. In 2009 second international conference on computer and electrical engineering (Vol. 2, pp. 431–435).

Kunyu, P., Jiande, Z., & Jing, Y. (2009). An identity authentication system based on mobile phone token. In 2009 ieee international conference on network infrastructure and digital content (p. 570-575). IEEE.

Kuo, C.-C., & Lo, M. (1999, December 14). Secure open smart card architecture. Google Patents. (US Patent 6,003,134)

Lance, S. (2019, June 27,). Time for password expiration to die (Vol. 2019) (No. 12/12/). Retrieved from https://www.sans.org/security-awareness-training/blog/time-password-expiration-die

Lehtonen, M., Michahelles, F., & Fleisch, E. (2007). Probabilistic approach for location-based authentication. In 1st international workshop on security for spontaneous interaction iwssi (Vol. 2007).

Li, C.-T., & Hwang, M.-S. (2010). An efficient biometrics-based remote user authentication scheme using

smart cards. Journal of Network and computer applications, 33 (1), 1–5.

Li, X., Niu, J., Khan, M. K., & Liao, J. (2013). An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications, 36 (5), 1365–1371.

Li, X., Niu, J.-W., Ma, J., Wang, W.-D., & Liu, C.-L. (2011). Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. Journal of network and computer applications, 34 (1), 73–79.

Li, X., Xiong, Y., Ma, J., & Wang, W. (2012). An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. Journal of Network and Computer Applications, 35 (2), 763–769.

Lim, C. H., & Kwon, T. (2006). Strong and robust rfid authentication enabling perfect ownership transfer. In International conference on information and communications security (p. 1-20). Springer.

Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. (2020). Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication. In 2020 ieee symposium on security and privacy (sp) (pp. 268–285).

Marforio, C., Masti, R. J., Soriente, C., Kostiainen, K., & Capkun, S. (2016). Hardened setup of personalized security indicators to counter phishing attacks in mobile banking. In Proceedings of the 6th workshop on security and privacy in smartphones and mobile devices (p. 83-92). ACM.

Medlin, B. D., Cazier, J. A., & Foulk, D. P. (2008). Analyzing the vulnerability of US hospitals to social engineering attacks: how many of your employees would share their password?. International Journal of Information Security and Privacy (IJISP), 2(3), 71-83.

Mishra, S., & Soni, D. (2019). Sms phishing and mitigation approaches. In 2019 twelfth international conference on contemporary computing (ic3) (p. 1-5). IEEE.

MLB9252. (2011, SEPTEMBER 24,). How to calculate pass- word entropy (Vol. 2020) (No. 29th June). Retrieved from https://ritcyberselfdefense.wordpress.com/2011/09/24/how-to-calculate-password-entropy/

Murthy, A. S., Ganesan, K., Mangam, P. M., Jandhyala, S. S., & Walter, M. (2020, January 28). Multifactor authentication as a network service. Google Patents. (US Patent 10,547,600)

Narayanan, A., & Shmatikov, V. (2005). Fast dictionary attacks on passwords using time-space tradeoff. In Proceedings of the 12th acm conference on computer and communications security (p. 364-372).

NCSC, (2019) Most hacked passwords revealed as uk cyber survey exposes gaps in online security (Vol. 2019) (No. 10/12/). (2019, 21 April). Retrieved from https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

ParthDutt. (n.d.). Understanding rainbow table attack (Vol. 2020) (No. 29th June). Retrieved from https://www.geeksforgeeks.org/understanding-rainbow-table-attack/

Poh, N., Bengio, S., & Korczak, J. (2002). A multi-sample multi-source model for biometric authentication. In Proceedings of the 12th ieee workshop on neural networks for signal processing (p. 375-384). IEEE.

Rayani, P. K., Bhushan, B., & Thakare, V. R. (2018). Multi-Layer Token Based Authentication Through Honey Password in Fog Computing. *International Journal of Fog Computing (IJFC)*, *1*(1), 50-62.

Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. World Applied Sciences Journal , 19 (4), 439-444.

Rouse, M. (2018, October). challenge-response authentication (Vol. 2020) (No. 01/09/). Retrieved from

https://searchsecurity.techtarget.com/definition/challenge-response-system

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11 (4), 89.
Salamatian, S., Huleihel, W., Beirami, A., Cohen, A., & M´edard, M. (2020). Centralized vs decentralized targeted brute-force attacks: Guessing with side-information. IEEE Transactions on Information Forensics and Security, 15 , 3749–3759.

Schneier, B. (2005, Mar 15,). The failure of two-factor authentication (Vol. 2020) (No. 29th June). Retrieved from https://www.schneier.com/blog/archives/2005/03/the_failure_of.html

Shablygin, E., Zakharov, V., Bolotov, O., & Scace, E. (2013). Token management. (US Patent US8555079B2)

Sharma, S. (2005). Location based authentication.

Shay, R., Komanduri, S., Durity, A. L., Huh, P. S., Mazurek, M. L., Segreti, S. M., . . . Cranor, L. F. (2014). Can long passwords be secure and usable? In Proceedings of the sigchi conference on human factors in computing systems (p. 2927-2936). ACM.

Simmons, M., & Lee, J. S. (2020). Catfishing: A look into online dating and impersonation. In International conference on human-computer interaction (p. 349-358). Springer.

Smith, N. (2018, 3 July). Hotp vs totp: What's the difference? (Vol. 2020) (No. 01/09/). Retrieved from https://www.microcosm.com/blog/hotp-totp-what-is-the-difference

Stasiukonis, S. (2006). Social engineering, the usb way. Dark Reading, 7.

Stephen, M. (2019, Jan 2,). Phishing attacks in the banking industry (Vol. 2019) (No. 16/12/). Retrieved from https://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demographic/phishing-in-the-banking-industry/

Thomas, B. (2017, Sep 18,). All that's needed to hack gmail and rob bitcoin: A name and a phone number (Vol. 2019) (No. 12/12/). Retrieved from https://www.forbes.com/sites/thomasbrewster/2017/09/18/ss7-google-coinbase-bitcoin-hack/#338f7a5f41a4

Tiwari, A., Sanyal, S., Abraham, A., Knapskog, S. J., & Sanyal, S. (2011). A multi-factor security protocol for wireless payment-secure web authentication using mobile devices. arXiv preprint arXiv:1111.3010 .

Tools, R. S. (n.d.). Password cracking tools (Vol. 2020) (No. 29th June). Retrieved from https://sites.google.com/site/reusablesec/Home/password-cracking-tools

Trojahn, M., & Marcus, P. (2012). Towards coupling user and device locations using biometrical authentication on smartphones. In 2012 international conference for internet technology and secured transactions (p. 736-741). IEEE.

Turnbull, R. S., & Gedge, R. (2012). Location based authentication. (US Patent US8321913B2)

Turner, D. M. (2016, 01 August). Digital authentication - the basics (Vol. 2020) (No. 16/05/). Retrieved from https://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics

Vel´asquez, I., Caro, A., & Rodr´ıguez, A. (2018). Authentication schemes and methods: A systematic literature review. Information and Software Technology, 94 , 30-37.

Weir, C. M. (2010). Using probabilistic techniques to aid in password cracking attacks.

Weir, M., Aggarwal, S., Medeiros, B. D., & Glodek, B. (2009). Password cracking using probabilistic context-free grammars. In 2009 30th ieee symposium on security and privacy (p. 391-405). IEEE.

Zhang, F., Kondoro, A., & Muftic, S. (2012). Location-based authentication and authorization using smart phones. In 2012 ieee 11th international conference on trust, security and privacy in computing and communications (p. 1285-1292). IEEE.

Zhang, L., Tan, C., & Yu, F. (2017). An improved rainbow table attack for long passwords. Procedia Computer Science, 107 , 47-52.