Passwords: the Weak Link in Digital Security

Strong Passwords and other Myths

Abstract

This white paper looks at the myths around strong passwords and the risk they pose to both service providers and their end-users who rely upon them.

SWIVEL

Contents

Contents

Executive summary

Web sites and online applications have become an integral part of everyday life. End-users now have so many online accounts, both personal and work related, it has become impossible for them to remember all their username and password combinations. This has led users to develop all manner of systems to remember them; from keeping hand written logs, to using the same password to access their accounts.

In addition, working practices have changed significantly over the course of the last decade. The advent of cloud computing, together with widespread adoption of remote working and bring your own device (BYOD) across the majority of industries, has led to an over-reliance on username/password security.

Password reuse has led to an epidemic of identity theft due to prolific data breach attacks specifically targeting end-user username/password combinations, an issue that is further exacerbated by the use of emails as usernames. Once this data is acquisitioned it opens the door to further attacks; just as the user does, the hacker can use the same combinations to gain access to other accounts.

Many service providers advise their end-users, often in response to a data breach, to create so called 'strong passwords' that consist of complicated alphanumeric and character sequences. However, there is increasing evidence that passwords are not enough to protect end-users from attack.

This whitepaper explores why those trading and operating in cyberspace have become reliant on username/password combinations, and how this issue poses considerable risk to both service providers and their end-users. It also identifies the different types of attack and the implications of these breaches. In response to these risks and vulnerabilities, the paper also highlights alternative authentication methods that can maintain the integrity of end-users' online accounts and therefore the sensitive personal and business critical information they hold.

1. Reliance on username and password

While service providers, for example, Amazon, Facebook, LinkedIn, online news sites etc., only require one username and password per customer, it is widely understood that end-users now have so many passwords to remember that it has become an impossible task to remember and recall them all. Indeed, a recent independent study revealed that nearly three-quarters (74.2%) of US business owners surveyed were keeping a written log or had an alternative offline system to record passwords.

The study also revealed that as recent as a decade ago, only 29.9% of business owners accessed more than 10 websites with a username and password. Today this figure has more than doubled to 61% as the number of online accounts and subscriptions held by end-users continues to grow and compound the password issue further.

1.1 The password explosion

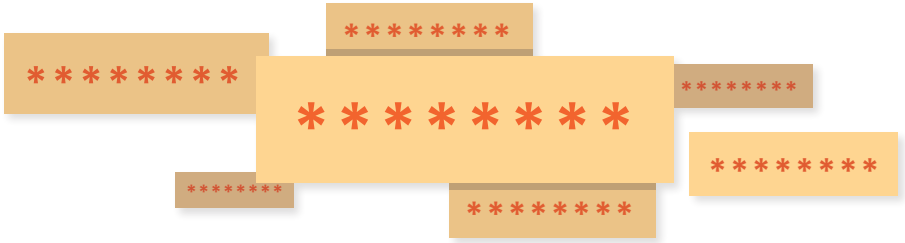
The requirement to create username and password combinations to access accounts continues to increase exponentially for a number of reasons. Online retail, banking and news sites together with other online subscriptions are continuing to gain traction with consumers. In addition, working practices are also a contributing factor, as a growing percentage of the workforce are able to work remotely, often using their own devices (BYOD) to access corporate networks via web-based or VPN connections. Many organizations are also opting to use cloud-based services to access applications and store corporate data, rather than hosting it themselves.

Increasing convergence between business and consumer applications – for example, cloud applications such as Dropbox, and social networks such as Facebook and Twitter being used as both business and personal platforms – results in the same username/password combinations being reused. In fact, according to the same study, 20% of respondents use the same passwords for both personal and business purposes.

This coupled with email addresses being utilized as usernames introduces multiple points of vulnerability, leaving both end-users and organizations equally vulnerable to attack. More than that, it is making it easy for hackers to successfully capture sensitive information.

Despite evidence to the contrary (which will be discussed in later sections of this whitepaper), username/password combinations are perceived to give an adequate level of protection against unauthorized entry and, as a result, remain the default process to access online accounts. The main reason for the reliance on this system is due to the familiarity of the process; it is the way that service providers and their customers have become accustomed to operating. This whitepaper will discuss why this process is now outdated and untenable, and more importantly, how it is leaving end-users and organizations at risk. It will also explore what the alternatives to the password are.

2. The consequences of password use



The password issue has been brought to the world's attention by a number of high profile data breaches that have been scrutinized by the media and other commentators, including attacks on global brands such as Google, Facebook, Twitter and LinkedIn, which have all resulted in end-users' details being compromised.

For example, in December 2013, US retail giant Target Corp suffered a major breach when it lost the personal details of approximately 40 million credit and debit card holders.

While earlier in 2014, Ebay experienced a data breach that exposed the site's 233 million customers' records, which included login information, leaving them critically exposed to identity theft. As a result, Ebay advised that all its end-users change their passwords, and in doing so, use 'strong passwords' which include upper and lower case letters, numbers and symbols.

Following this breach, Ebay reportedly suffered huge financial and reputational losses as it failed to attract new users and found itself losing revenue as well as facing regulatory fines. It was also heavily criticized for having weak security measures in place.

Ebay is not alone in advising its users to reset and use strong passwords following a breach. This whitepaper explores the validity of this advice and whether the use of strong passwords for all online accounts is the right course of action.

2.1 The implications of a breach

As a result of these high profile incidents, more businesses and organizations are putting data leak prevention strategies in to place as they realize they are not immune to breaches. Every organization has business critical and sensitive data; whether it is intellectual property, financial information or employee records, which they have a duty of care to keep secure.

The consequences to those responsible for such data leaks can be catastrophic in terms of reputational and financial losses, such as imposed fines and lost revenue. According to the Ponemon Institute's '2014 cost of a data breach' study, it is estimated that each record lost comes at a cost to the business of $145, and the average total cost of a data breach is $3.5million, a rise of 15% compared to 2013's study.

2.2 Different types of data breach

There are many data breaches which involve the hacking of organizations in order to get possession of personal records which include user and password information. This information can then be used for other types of attacks and ultimately for financial gain.

There are a number of different types of hackers and methods they use in order to retrieve this information.

2.2.1 Categories of hackers

- **The ethical hacker**, also known as **the white hat** – tends to be someone that works in the security industry and is testing his/her skills and may perform vulnerability and penetration tests for a job.
- **Cracker** or **black hat** – is someone that has malicious intent and is an expert in cybercrime including fraud and identity theft. This type of hacker will employ different tactics to get the data they need including phishing, Trojans and password attacks.
- **Grey hat** – this type of hacker has traits of both the ethical hacker and the cracker. They will use their hacking skills to search for vulnerabilities, and when they find them, offer to resolve any issues and charge the organization at risk.
- **Script kiddie** – uses packaged scripts they find on the internet to hack. They are not expert hackers and have little technical ability.
- **Elite hacker** – these hackers are renowned in the criminal underworld for being the best at what they do. Some elite hackers, once penalized, will retire from crime and be employed by legitimate organizations to help develop security solutions and strategies.
- **The ordinary person turned hacker** - it is important to highlight that not all data breaches are masterminded by professionals and criminal gangs. It could be just about anyone; from a disgruntled employee, to a family member, to a patient that has suffered medical negligence, for example. The proliferation of hacking tools means that many attacks can be implemented with a small amount of expertise, especially if the attacker has some form of privileged access to the target network.

2.2.2 Different types of attack

There are many different ways to hack or attack a system, this whitepaper concentrates specifically on those that exploit passwords.

- **Dictionary/brute force/hybrid attack** – all are password attacks. The dictionary attack uses a list of passwords to try and gain access. The brute force attack uses every combination of characters to try and gain access. The hybrid attack is a combined dictionary and brute force attack.
- **Phishing attack** - this involves the hacker creating a website identical to legitimate sites, e.g. a bank, and then sending an email to end-users which attempts to trick them into inputting username and password details which the hacker can then capture and use in other attacks.

- **Passive attack** – this attack monitors network traffic and looks for clear text passwords and other sensitive information that could be useful in other types of attacks.
- **Active attack** – this type of hack actively tries to break into secured systems by various means including Trojans, viruses and worms. Its aim is to introduce malicious code that will either capture or modify data. This type of attack can result in the disclosure of sensitive information, including passwords which can be used in other attacks, and also often results in denial of service (DoS).
- **Distributed attack** – this attack introduces malicious code, often through the backdoor, by a Trojan for example, which will gain access to sensitive information including passwords and other business critical data.
- **Man in the middle** or **fire brigade attack** – this attack is characterized by the hacker listening in to communications between two parties, which is then modified by the hacker without either party realizing. This method of attack can 'sniff' out all types of data including passwords.

It is important to note that many breaches can be the result of businesses and their staff not securing sensitive information adequately or not adhering to security policies; for example, saving data onto USBs, printing out documents or emailing data to private accounts.

How attacks operate in real world scenarios

The 2013 attack on retailer Target resulted in a data breach on a previously unprecedented scale. A significant proportion of the population was affected – in the region of 110 million people – but it also impacted Target's partners including MasterCard and Visa, and as a consequence the black market was flooded with high value cards as a result of identity theft using the stolen data.

This data breach could also have resulted in highly targeted attacks including phishing, where tailored emails could be sent to end-users using the stolen data to gain access to end-users' systems. It was also reported by the New York Times that although Target took steps to protect end-user payment information, the triple DES encryption algorithm used was vulnerable to brute force attacks.

The impact on Target has been significant as damage to both its reputation and bottom line have been substantial.

In many cases, the number of users affected by a data breach is difficult to calculate as the consequences of such action isn't understood for months following an attack.

3. The critical issue of prolific password reuse

Password reuse is serving to increase the vulnerability of end-users and organizations to attacks. Both strong and weak sequences are commonplace as end-users struggle to remember multiple access details. This reuse of passwords further weakens security as the compromise of one website makes other sites using the same username/password combinations easy targets for hackers.

For example, Best Buy accounts were attacked using credentials stolen from another website, which the retail organization was reportedly unaware of for months despite its customers complaining of compromised accounts. The value of stolen data on the black market increases substantially when financial information such as bank details can be accessed.

As already discussed, many organizations that experience a data breach will advise their end-users to change their passwords to so called 'strong' passwords. There is evidence, however, that this advice is often not followed. The top 10 passwords used, for example, are simple sequences. In addition, a study from one of the world's largest organizations Microsoft, argues that weak passwords have their place (see section 3.2).

The reuse and inherent weakness of both strong and weak passwords as a means of access to accounts calls into question their viability as an authentication method in any circumstance. The types of attacks described in section two illustrate that there are many ways to get access to sensitive personal data and business critical information by targeting passwords alone. Section four explores the alternative authentication methods available.

3.1 Strong passwords

Strong passwords are defined as being at least eight characters long, and a mix of upper and lower case letters, numbers and symbols. Many service providers advise end-users to use strong passwords and will indicate their strength when opening accounts, for example, weak, adequate, good or strong. If an unauthorized user or attacker is trying to gain access to an account, after a predetermined number of failed attempts the account will be locked. For this reason, an attacker will try common passwords first, so it is important for the end-user to avoid using popular passwords.

However, while strong passwords may prevent colleagues, friends and family from accessing accounts, they are very unlikely to prevent a serious hacker gaining entry. For example, if a website is compromised, the strong passwords are captured along with the weak, and therefore leaves all users equally vulnerable.

In addition, the thing that makes strong passwords strong is, paradoxically, also what makes them weak, thanks to the sheer number of complicated sequences end-users are expected to remember. As this is an impossible task, end users have little option but to adopt strategies such as recording their passwords offline, or to use the same password for every account they have.

3.2 **Weak passwords**

It is easier for end-users to recall a weak password as they are simple, uncomplicated sequences. However, it is still an impossible challenge to remember a high number of weak passwords, which again leads to their reuse or to users recording them offline. In addition to reuse by a single end-user, multiple end-users often unwittingly share the same weak passwords.

In July 2014, Microsoft and Carleton University revealed the results of a study that advised users to use and reuse weak passwords for websites that do not hold high value information, such as bank details and other sensitive information, which could be used for identity theft. It argued that this will allow end-users to remember complex passwords for the sites that warranted the additional security, such as banking and ecommerce sites.

Most popular passwords

In spite of the advice to use strong passwords, the top 10 most popular passwords used (source: SplashData) gives an insight into the uncomplicated sequences favored by end-users. The inspiration for many passwords includes pet and family members' names, birthdays and dates of other special occasions, the name of the application it is used to access e.g. photoshop, and easy to remember numerical or alphabetical sequences.

The top 10 is:

123456	123456789
password	111111
12345678	1234567
qwerty	iloveyou
abc123	adobe123

4. Alternatives to using passwords

As the increasing number of high profile data breaches serve to highlight how end-user passwords are targeted in order to coordinate further attacks, it calls into question the validity of using passwords alone to access online accounts. Passwords are the weak chink in security's armor, but there are a number of alternative technologies and methods which bypass the need to use conventional passwords and offer far greater protection for service providers and end-users.

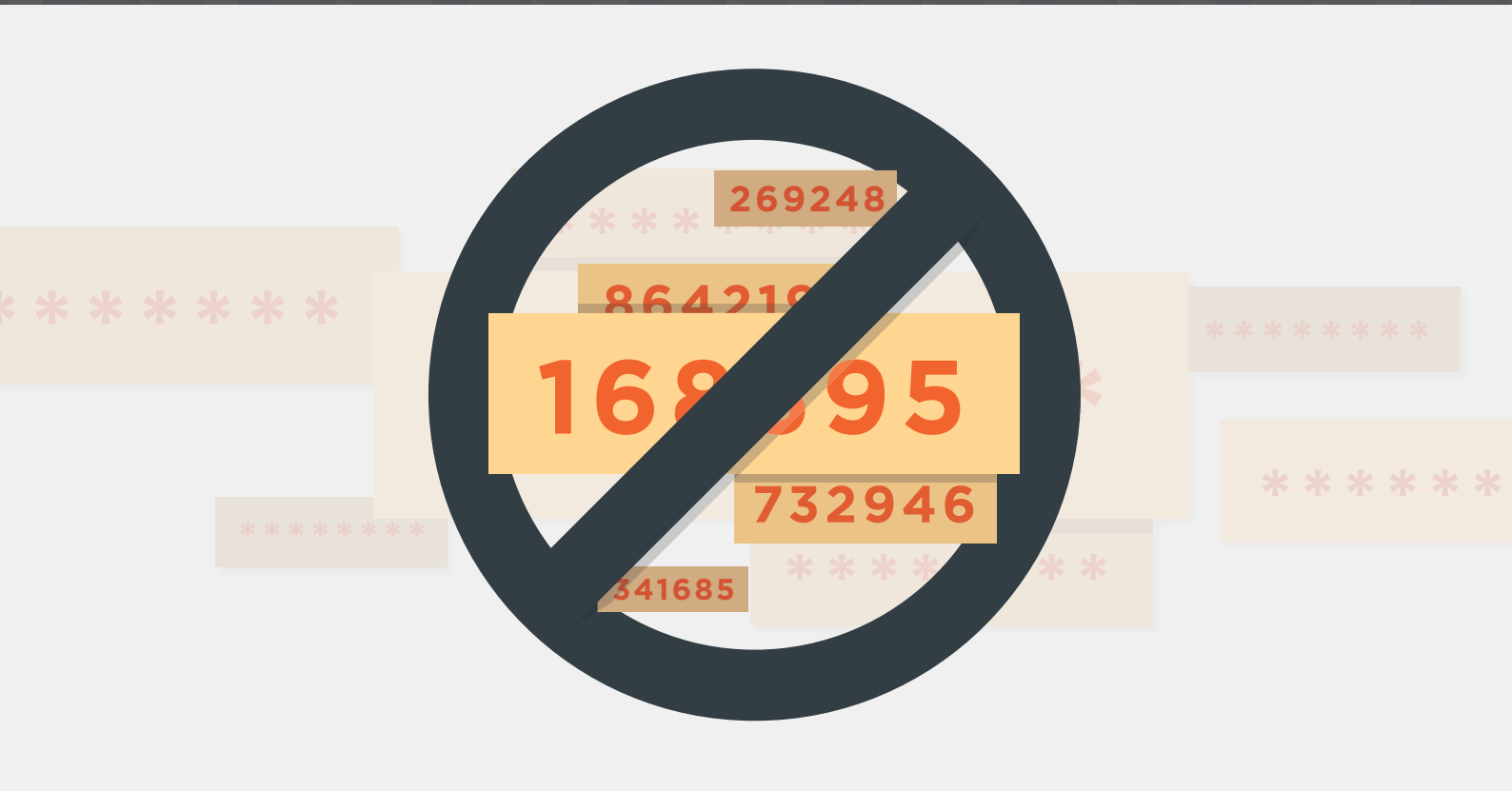
There are a number of elements that can be used to authenticate a user. These include information that is created by the end-user (something they know) e.g. passwords, secret answers such as mother's maiden name, and passphrases; physical features that can be used to recognize them which are unique to each individual e.g. iris, fingerprint, face; or physical tokens (something they have) including chips and USB keys.

There a number of drivers that are leading service providers to consider alternative authentication methods as the issue is becoming even harder to ignore, and more and more sensitive information is being held in password protected accounts vulnerable to attack. However, the uptake of these technologies is still remarkably slow considering what is at stake for all involved in using and delivering online services.

The following authentication methods can all play a role in verifying end-users and protecting against identity theft:

4.1 Token-based authentication

Authentication of users is determined using two different components which includes something the user knows, for example, a password, and something they possess (the token), for example, a USB key or a card. The user must demonstrate that they know the password and have the token to be granted access to specific resources. Both must be correct and established beyond doubt in order for authentication to be verified. This type of authentication means that the end-user doesn't have to share their username and password. The drawback of this technology is that if a token is lost or simply not on the user's person at the time of login, access is denied.



4.2 **Tokenless two factor authentication**

This technology was developed to overcome the shortcomings of token-based authentication. As is the case with token-based authentication, tokenless two factor authentication is determined using two different components. However, this technology negates the need to have a specific additional token such as a card or key, as it uses an app on the user's smartphone to generate a one-time code, or can send this in an SMS or email. This one time code will become invalidated based on time or on an event e.g. it is used. In order to authenticate the user, they must use something they know, for example, a personal access code, along with this dynamic passcode.

4.3 **Multi factor authentication (MFA) also known as two factor authentication (2FA)**

Not to be confused with strong authentication, multi-factor (MFA) or two factor authentication (2FA) requires the use of two or more authentication factors from different categories as follows in order to gain access to an account: something they know, something they possess and something that they are. Using multiple factors from the same category would therefore not constitute MFA/2FA.

4.4 **Strong authentication**

Similar to MFA or 2FA, strong authentication, also known as stronger authentication or strong customer authentication, requires two or more authentication factors from the following categories: something they know, something they own and something they are. The difference to MFA/2FA is that the factors selected must be mutually independent, i.e. the breach of one will not compromise another factor. In some instances of strong authentication requirements include a non-reusable and non-replicable factor. This method is often used by the heavily regulated financial and banking industry in order to make remote payment transactions.

4.5 **Biometrics**

Biometrics uses physical features which are unique to the end-user including facial recognition, iris recognition, fingerprint recognition and even palm vein patterns in order to verify and authenticate an end-user. It is a technology that is still considered to be emerging by some. However, this technology is being deployed in a number of areas including the use of fingerprints to access smartphones, and airports are increasingly adopting different types of biometric recognition as they look to strengthen security. Some mobile phone-based biometric solutions for enterprises are beginning to come to market.

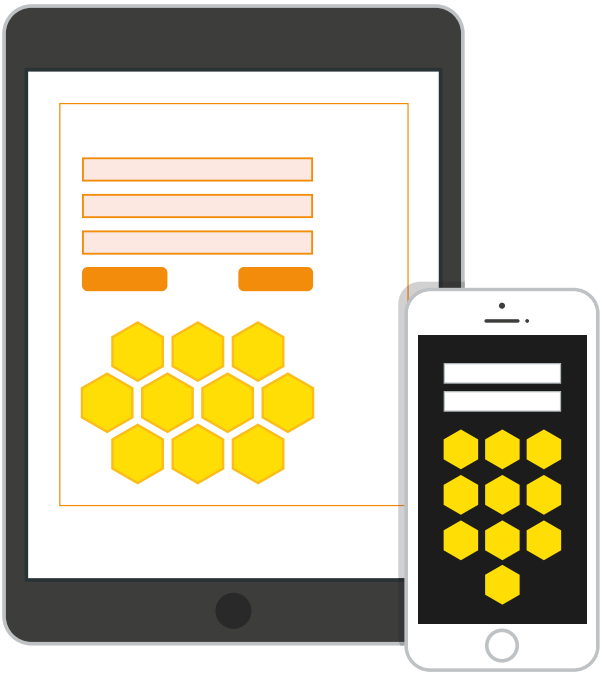
4.6 **Password management tools**

It should be noted that tools exist to allow end-users to use strong passwords without having to remember them. Software generates a password in encrypted form and all the end-user has to remember is one 'master' password. However, though these tools address the reuse issue to a modest extent, they have many limitations, including the fact that if the master password is cracked, it opens the gate for the hacker.

5. Can service providers afford not to step up authentication?

The high profile data breaches have demonstrated that the strong password does not exist. When data is hacked, the strong passwords are acquisitioned along with the weak. In addition, using weak passwords for accounts that are perceived to hold non-sensitive information is a high risk strategy to adopt. As this whitepaper has established, the critical issue of prolific password reuse means that the capture of one password will often unlock multiple other accounts that hold additional sensitive data.

There is mounting evidence that username/password combinations are not enough to maintain the integrity of personal and business critical information. The time has come for service providers to embrace alternative technologies, such as the financial and banking industry has, in order to better serve their end-users.



Using authentication methods that require factors that include *what you know*, *what you own* and *what you are*, mean that passwords are no longer necessary, and even if a password is one of the authentication factors, it cannot unlock accounts by itself.

Adopting these methodologies would dramatically decrease identity theft, which is expected to surpass traditional theft, as the rewards to the hackers are high as username/passwords are highly lucrative. It is also important to highlight the often devastating impact these anonymous online crimes have on the victims.

As adoption of online services continues to increase, service providers cannot afford to overlook the security and authentication of their end-users. They have a duty of care.

6. About Swivel Secure

Established in 2000, Swivel is a pioneering network security solutions provider. Its multi-factor authentication platform, underpinned by PINsafe, the company's patented one-time-code extraction technology, is recognized as the de facto standard in tokenless authentication technology.

Swivel's established user base includes major blue chip companies as well as SME and public sector organizations. Customers vary from UK NHS Trusts to multi-national logistics organizations, high street retailers, financial institutions and one of the world's largest IT hardware components manufacturers.

Swivel is the only authentication technology accredited for Microsoft Office365, which offers primary support for a tokenless environment.

Swivel has an extensive world-wide network of channel partners and is a member of Marr T&T, the technology arm of the Marr Group, a global investment business.

For more information on its multi-factor authentication platform, please visit or get in touch.

SWIVEL