DXC.technology

White Paper

The problem with P4$$WORDS!

How to improve the most common form of authentication

Passwords are almost universally used as the primary means of authenticating the identity of a person for computer systems or applications. They may come in different forms — such as alphanumeric text, PIN digits, passphrases or "select A from B" systems — but they all share the same characteristics.

Passwords are a string of symbols that users memorise and keep secret. The string must be entered correctly to authenticate and allow access (subject to authorisation, which is not being discussed here). Failure to enter the password correctly implies that the identity is not authenticated, but a failure does not distinguish between error and attack. Instead, a sequence of failures is normally viewed as an indication of an attack, and the normal response is to temporarily disable the account, or perhaps delay the response to each new attempt

This paper will show that passwords provide a sense of security that can be highly misleading. Security professionals agree that although authentication by password alone is used the vast majority of the time across the Internet and in enterprises, more robust authentication systems provide better protection.

Organisational impact

Authentication systems can have a significant impact on an organisation's operations. In a world where outsourcing is increasingly the norm, and where Software as a Service (SaaS) solutions, single sign-on and federated identities have become common, the service management issues of identity and authentication take on a more visible and critical significance. They also become external costs and therefore visible to the organisation.

As a global IT services provider, DXC Technology has found that up to one-third of all service desk requests at peak periods may be the result of password-related issues. Over an 18-month period, 15% of service tickets are password related. There is no obvious correlation between the requests and the type of system being used, although having multiple systems can have an effect. In one extreme case, 60% of all service desk tickets arose from password resets, which could have been due to the combination of a 60-day password change policy and the existence of multiple authentication systems.

DXC has also found that technology solutions can cause unintended problems. Without careful planning and architecture for authentication systems, issues with synchronisation become visible and can cause account lockout. Automated password reset systems address the symptom rather than the problem. Whilst automation reduces the number of service tickets (and the visible cost associated with them), users need to know what they are doing. Automated systems may not improve the speed of resolution, which can maintain, or perhaps worsen, the invisible cost impact.

Cost implications can be potentially huge. An organisation incurs visible costs through the processing charge for a ticket, but the productivity impact of an employee being unable to work can carry a higher cost. If a password reset process takes 30 minutes from the user-experience perspective (the service-desk perspective is a lot shorter), then the impact on the user is high. And, of course, it seems password issues happen only when there's time-critical work to be done.

Organisations will want to address both the security of their environment and the cost to maintain that security. As with all things, this becomes a balance of cost versus risk. Three factors affect this balance:

- Password policy: complexity and frequency of change
- Multiple systems: number of passwords to remember
- Recovery process: accessibility and response time

An organisation must balance these factors to achieve an acceptable level of risk versus the cost of maintaining the security level. Each organisation will need to determine that balance point based on its own understanding of the risks and threats. DXC usually suggests that some strategic investment can provide a long-term improvement in risk, whilst simplifying the user experience and reducing the visible and invisible impact of password failure.

When weighing these factors, bear in mind:

- Increased password complexity allows reduced change frequency.
- Multi-factor authentication reduces change frequency AND increases security.
- Single sign-on reduces complexity and password failure.
- Passwords on their own do not constitute sufficient security for many activities.
- Password recovery must be as secure as the asset the password is protecting.

The attacker's view

Attackers like passwords. Besides being relatively simple to obtain, passwords often provide easy access to information.

Hackers are in a race to find vulnerabilities before defences can respond. Zero-day vulnerabilities that result in information breaches cost money to find, develop and exploit in practice. In a remote attack, there are many layers of defence between hackers and their targets. But if the attacker has access to passwords, those defences crumble very quickly — and, worse, the activity looks legitimate. The defences can be further compromised to facilitate future use.

Category	Typical Attack Vector	Standard Defences	Effectiveness of Password Complexity	Effectiveness of Password Change
Social Engineering	• Phishing • Shoulder surfing • Social media	• Physical security • Email and Web usage controls • Awareness	• Low	• Low, as password is available to attacker very quickly
Mechanical	• Hash tables • Brute force	• Increasing time-out • Account lockout • Cryptography	• Increases with high complexity and entropy • Effectively, low if offline attack available	• Increases with frequency of change
Stealing	• Exploiting poor storage and handling	• Policy against written passwords • Policy against scripted passwords • Password vault	• None	• Increases with frequency of change
Technical	• Keylogging • Interception	• Anti-malware • Encryption during transmission	• None	• Low, as password is gained in real time and can be used immediately

As a result, much of attackers' energy goes towards attempting to recover passwords. There are many ways they can do this, but the approaches fall into a small number of categories and attack vectors, each of which has a corresponding set of standard defences. The following table shows that password policies can be of limited use.

What's notable is that password complexity and expiry controls do not have a significant impact against the attacker when one considers the number of attack routes that can be exploited. What is needed to properly defend against attacks on authentication is a variety of controls, including:

- Password controls
- Multi-factor authentication
- Anti-malware controls
- Privileged access controls
- User education
- Activity monitoring
- Effective monitoring of the environment

Effective use of these controls can reduce the importance of the classic password. This does not mean that password controls should not be used; but as passwords become less important, the risk is reduced, the user experience is improved and the cost of security to the business — in time lost and in IT requests — is also reduced.

Faced with a well-managed combination of the controls above, attackers have a much more difficult time exploiting a system. They must exploit vulnerabilities in the software rather than the people, which is more expensive and time consuming, and results in a reduced chance of a successful outcome.

Examining the mathematics

Passwords are strings of characters, and their strength is linked to their randomness, something measured by entropy. For our purposes, say that password strength can be increased in two ways:

- Increasing the number of characters in the set from which the password can be chosen (e.g., changing from using only the alphabet to using the alphabet plus numeric characters adds 10 options)
- Increasing the length of the password

As an example:

A password of eight characters selected from 26 letters (the alphabet) will have 26^8 (208,827,064,576) possible solutions. By adding numeric characters to that set, we get to 36^8 (2,821,109,907,460) solutions, about 13.5 times as many.

By increasing the password length to nine characters, and just using the alphabet, we go to 26^9 (542,950,367,898) possible passwords, which is clearly 26 times more than the eight-character option, and more than double the shorter password from the wider character set.

We can see, therefore, that increasing password length has the greatest impact on password strength. This is where the passphrase idea comes from. Supporting and requiring longer passwords — normally by suggesting that individuals use a phrase, such as "mycookingisawful" — results in an exponential increase in password strength. Note that older operating systems, and even some current ones, would allow the entry of long passwords, but ignore anything after a certain number of characters (eight, in the case of UNIX), severely limiting the possibilities.

People and language

"Password" is commonly found to be the most common password in surveys or rainbow tables. Mathematically, in any given character set, "Password" is as strong as any other eight-character string — that is, it has equal probability of appearing in any random selection of eight characters from the set. But it illustrates a big problem.

People will choose passwords that they can a) remember and b) type easily. From a given character set, this means that people will normally tend towards using words in their own language and will further constrain the selection by choosing words that are meaningful to them. This quickly reduces the randomness (entropy) of the passwords chosen.

A quick look at some online Scrabble dictionaries (which don't include proper names) shows approximately 40,000 (a little over 26^3) eight-letter words in the English language. That's a small fraction of the possible character combinations, and the average user only knows a small proportion of those words.

It is worth noting that breaking up passwords into combinations of words (two four-letter words, for example) increases the possible combinations drastically, whilst retaining the memorability. This supports the idea of the passphrase being superior to the password.

Considering that users need passwords to be memorable, which further constrains their likely selections, the risk of a password becoming guessable increases. Find out a little about the individual — now easy to do with social media platforms — and the possibility of an attacker determining a password becomes more likely. Children, middle names, spouse names, favourite sports team all get used as passwords or as the basis for a password.

The only defences against weak passwords are maximum-attempt lockouts and strong cryptography in the password store. But with an intelligent and advanced attack, passwords still remain very high on the list of potential vulnerabilities an organisation faces — in many areas, second only to the inside attack.

Making it a little more difficult

Knowing users' password preferences, organisations do three things, usually in combination:

1. Increase the minimum password length
2. Increase the number of characters (symbols) in the pool; including numbers and special characters is standard practic
3. Specify minimum combinations of symbol types that must be used (e.g., three uppercase, lowercase, numbers, symbols)

The practice of requiring that passwords can't be re-used within a certain time period or within a set number of changes is also common.

Increasing the length and variety of possible combinations may increase potential password strength. A UK QWERTY keyboard has about 100 symbols directly available, and a knowledgeable user can use key combinations to come up with further symbols. Moving to a 12-character password in a 100-symbol context gives password possibilities of 100^{12}, which is a few billion times larger than the eight-character, alphabet-only password.

But moving to longer passwords creates a more difficult memory issue. To address this problem, the individual can use a phrase (there aren't many well-known 14-character words). Passphrases assist password strength by introducing semi-randomness into the selection. Memorable phrases can be nonsensical, yet familiar. They can be very personal and yet not related to information in the public domain.

However, studies show the average individual uses a very small number of words and phrases in daily life, so the selection problem is a threat to password strength even in a passphrase (long password) environment. By tending to use phrases from normal and natural language, and moreover choosing phrases that are memorable and perhaps familiar, the randomness, and hence the password strength, is reduced.

One security response is to force people to use passwords that have increased complexity, lowering the direct relationship to known words or phrases. By forcing the use of combinations of character types, employees are pushed away from using natural language. This increases the actual password strength, but paradoxically, reduces the overall entropy (strength) of the system in use in two ways. First, it actually reduces the number of possible combinations that may be used. Second, as people tend to use certain patterns in an attempt to retain memorability, those patterns are often predictable.

Here's an example:

Alice would like to use the word "password" as her password. The system uses upper case (26) and lower case (26) characters, numbers (10) and symbols (38), and requires 10 characters, giving a natural strength of 100^{10} possible combinations. The policy requires that Alice use each of the possible symbol types. As a result, the possible natural strength has now decreased, as four of the characters have to be chosen from a limited set and three from the entire set. This results in $26*26*10*38*100^{7}$ combinations, which is approximately one-quarter of the natural strength, although still a very large number.

Alice, however, needs to remember the password. “H&*1nf)d” doesn’t seem easy. Something close to her memorable word will be better. So she chooses “Pa55word!!”, which meets all the requirements for complexity, length and her own personal requirement of memorability.

The attacker has a harder task. The possible combinations are much larger, but because of human nature, the password is still easier to break. People tend to map symbols and numbers to replace letters. It can be seen that the number of ways “password” can be remapped to be memorable and easy to type is relatively small. Thus, forcing a combination of symbol types hasn’t significantly increased security.

Forcing change

Knowing that attackers will be able to exploit human nature, organisations often react by putting time limitations on passwords, forcing users to change them on a regular basis. Typically, an organisation will implement this strategy on a two-tier basis — that is, normal identities change less frequently than those with significant privileges.

Yet forcing password change has little upside, for a number of reasons:

- Increased change rate will increase the password support-ticket rate (and therefore, the cost) as people forget new passwords or find themselves locked out.
- People will resist the change by selecting new passwords that are similar to the old ones, typically done by incrementing a number or adding a repeating symbol (“Pa55word1!” goes to “Pa55word2!”). As this action is relatively predictable, an attacker could assume a comparatively small set of possibilities for the new password, based on some knowledge of the original.
- People have many passwords, and changing them causes memorisation issues. This drives poor user behaviour, such as writing the passwords down.
- Changing a password based on time or frequency of use leaves a window of trust where the organisation is effectively assuming the password is secure. If a change is required every 6 months, the assumption is that the password is safe enough for 6 months. Yet the password could be at its most vulnerable during that time. Perhaps Alice has written it down to help her remember it, or perhaps there’s an expectation in IT support that the password will be forgotten, so there are less-stringent common practices around password reset requests.
- Shared passwords (for generic, often privileged accounts) many times are not changed according to schedule, which means:
    - Privileged accounts are paradoxically more vulnerable.
    - Emergency use of privileged accounts may be impeded because of forced password change, just when you’re trying to log in.
    - Password changes may not be recorded properly, causing issues for later access attempts.

Password policy

Before thinking about the technology of passwords, it's worth remembering that, as shown, passwords are a people problem as much as a technology one. An organisation must have a password policy that educates about and emphasises the importance of password safety, as well as stating certain rules that individuals should follow (and are difficult to enforce technically).

Rules should include the following:

- Don't share passwords.
- Don't write passwords down or store them insecurely.
- Don't re-use passwords.
- Use different passwords at work than you do at home.
- Use different passwords on different systems and applications.
- Use different passwords when working at different privilege levels

The previous sections have shown that passwords are an inherently weak form of authentication for many reasons. Often people are the biggest factor in that weakness. Technical solutions, such as single sign-on (SSO), mitigate the user impact, but the lack of a single public SSO system means that users have many passwords for both work and personal use, which increases the "bad" behaviour. Personal password-vault solutions make things easier, but introduce availability risk.

Any solution that affects usability increases risk to the user and the organisation. As the ultimate solution, SSO allows users to minimise the number of passwords and therefore lets the organisation increase the frequency of change. But now the attacker only has to find one password to access many systems — whereas before, there was separation and then a boundary to risk.

Password policies — an organisation's rules about length, complexity and use of passwords — are the best way to balance risk and user impact. Every organisation should consider how to set that balance for its environment by weighing the following:

- Sensitivity and value of the asset being protected
- Capability of the identity being authenticated
- Password solution and reset process
- Impact of password failure on the business
- Capability of the password solution for password standards enforcement
- Culture of the organisation
- Regulatory and legislative requirements

A typical password standard may have a two-tier or a three-tier approach:

1. Privileged accounts

a. Length: Minimum 15 characters[1]

b. Complexity: Three from four categories[2]

c. Re-use: None

d. Change: 30 days

2. Standard accounts

a. Length: Minimum 12 characters

b. Complexity: Three from four categories

c. Re-use: Not in last 10 passwords

d. Change: 180 days

3. Guest accounts

a. Length: Minimum eight characters

b. Complexity: None

c. Re-use: None

d. Change: Per guest

Additionally, organisations should consider implementing some or all of the following controls, if possible:

- Reject "similar" passwords — where the new password is compared against the previous password and checked for similarity. This avoids the incrementing-password problem — when, for example, "Pa55word!!1" becomes "Pa55word!!2".
- Gradually increase the time required between login attempts before account lockout to prevent throttling.
- Provide approved password storage systems.

Reference Policies and Information Sites — Examples

A number of reference policies and information sites are available, including some from government and related agencies that discuss the use of passwords. While one should verify whether one's own local government or preferred standards body has made any recommendations, here are some examples:

- **UK government (CESG) recommendations**

  https://www.cesg.gov.uk/topics/passwords

  This site includes a variety of useful infographics, policy recommendations and, of particular interest, background as to why CESG (originally, Communications-Electronics Security Group) is currently discussing the benefits and issues of enforcing regular password change.

[1] Note: Some systems or applications may not support longer passwords.

[2] Note: Some environments may not support certain complexity requirements.

- **NIST password recommendations**

  http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-10/oct23_choong_password.pdf

  The National Institute of Standards and Technology (NIST) [U.S. Department of Commerce] has provided a number of statements on password usage. This presentation gives some interesting background on password policies versus actual user password selection.

  http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-63--3

  SP-800-63 is, at the time of writing, in public consultation draft (version 3). The history of this document includes a specific password document, SP 800-118, which is unfortunately no longer available from the NIST website.

- **SANS password policy**

  https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

  This industry-standard reference document forms part of a suite of policies available free from the SANS Institute.

When it fails

Even a perfect system will suffer from password failures. People returning from extended time off, “finger trouble”, accidental keyboard re-mapping and other factors all combine to drive a minimum failure rate.

The organisation’s goal when a password fails is to minimise both the visible cost of recovery and the user impact. Of these, the greater cost is the user impact. A nominal ticket resolution charge for password reset is insignificant compared to the impact of a 30-minute outage for a senior employee, especially when there are knock-on effects such as missed deadlines.

To remedy this, a simple and easily accessible password reset process is necessary. Self-service solutions remove the unit cost from the service desk, but these depend on the user’s being able to access the environment sufficiently. This may not be possible if the user is locked out of the environment.

Not all systems are able to support self-service solutions, so the organisation will need to develop a password reset process that maintains the security of the environment protected by that password — assuring that individual’s identity and using appropriate reset mechanisms.

But passwords aren’t enough

As shown in this paper, the mathematics of passwords are good, but the human issues make relying on them a serious concern — especially in cases of higher-risk environments, privileged access, sensitive data or remote access. Eradicating passwords is not necessary, but an organisation should seriously consider the use of additional authentication mechanisms to control risk in these areas.

The insider threat is often viewed as the most obvious risk to an organisation, but tied to this is the fact that almost all technical vulnerabilities and attack paths require the compromise of a privileged account. By strengthening controls around the use and management of privileged accounts, the risk can be strongly mitigated, regulation compliance can be achieved and better business processes can be introduced.

DXC recommends that organisations consider implementing the following controls at appropriate points in the environment:

Privileged access control

Privileged users of systems, devices and applications have the ability to deliberately or accidentally cause loss of data availability or compromise sensitive and important data. Privileged accounts are the attacker's ultimate target, as these accounts allow access under the guise of an authorised account.

Role-based access control ensures that individuals have the necessary access for their roles without improving the risk profile of the authentication system. A password-control system (such as that provided by CyberArk) hides passwords from the user for privileged accounts, forcing a very high level of password security (randomness) and requiring users to use multi-factor authentication. Both account use and use of the privileges associated with the account are monitored and recorded, and may be reported and audited.

Generic and shared account management

Generic and shared accounts (including the default administrator account built into almost all devices and systems) are often the most sensitive, privileged and neglected of all accounts. These accounts must often be used by many individuals, which therefore demands password sharing — with all of the risks that implies. Because of that shared environment, password change compliance can be very costly and difficult to achieve, and is often neglected.

A standard approach to mitigating this problem is to use privilege escalation within the system (e.g., Sudo on a UNIX or Linux system). However, this merely shifts the risk rather than reducing it. With this approach, access control relies entirely on a local text file containing authorised users, and the password remains the sole authentication for the normal user account.

As with privileged access control, a password control system (such as CyberArk) can eliminate many of the issues arising from shared accounts. Passwords no longer need to be shared, can be demonstrated to be highly secure and can be managed appropriately through an automated system.

Multi-factor authentication

Multi-factor authentication requires a number of authentication tools, one of which, ideally, is cryptographically strong. In a typical multi-factor approach, the user has an identity (e.g., Alice@widgets.com), a password (something she knows) and a token (something she has).

This approach mitigates password compromise: For an attack to succeed, the attacker needs access to the token (which may itself require a password or personal identification number [PIN]), as well as the password. Tokens are often either hardware or software-based, tied to something like a mobile phone. Software tokens are growing in popularity due to the administrative simplicity, low cost in distribution and management, and availability of cloud-based SaaS solutions.

A significant benefit is that Alice can tell right away whether her token (phone) has been lost, and she is able to raise an alert much sooner, reducing the risk and impact of an incident. Conversely, she can't know whether her password has been compromised. Multi-factor authentication therefore provides stronger access control and faster detection of a potential compromise. It is strongly recommended for use in accessing sensitive systems, data, network control points and for remote access from untrusted networks into the organisation's corporate environment.

Single sign-on

As discussed earlier, SSO solutions provide user benefit whilst potentially compromising any system supported by the service. SSO solutions do, however, offer other advantages in access control, including the ability to easily shut down an individual user across multiple systems from a central point.

Use of SSO should be considered carefully in the context of the system's sensitivity and the user's privileges. SSO systems can be combined with multi-factor authentication to provide the best of both worlds, and they are a good compromise for users. However, for privileged access, the recommendation stands that a separate system be used to provide stronger levels of control, compliance and monitoring.

Identity and access management review

Authentication, whether through passwords or a multi-factor system, is the process of assessing whether users are who they claim to be. It must be tied in with two processes that are equally important in providing end-to-end control:

- Identity management
- Access management

Identity management is the process of ensuring that the people and entities that have access to the environment at any level are valid. This process should be tied into a Human Resources management system, as well as procurement processes for third-party services. Frequent and regular review of such lists, along with appropriate processes for adding and removing names, is crucial to preventing an individual from maintaining perpetual access to a system beyond what's required by the organisation. An account that continues to exist after an individual leaves an organisation will not have appropriate password changes and introduces a high degree of risk for the organisation and a valued target for an attacker.

Access management is the process of ensuring that a valid identity (as shown by the identity management process) has access to the systems and data appropriate for the role, and that access is properly authorised and terminated when necessary. An account that accumulates privileges over a period of time, yet is subject only to password controls, increases organisational risk considerably, and this housekeeping process mitigates that risk.

Many tools exist to support a high degree of automation in these processes, which are often required to achieve regulatory compliance.

Looking ahead

The classic password approach to authentication has many weaknesses, the biggest being the human element. Many organisational attempts to increase password strength do not have the desired effect because of user preferences and limitations. SSO solutions support the user in the struggle to remember multiple passwords, but expose the organisation to other kinds of risk.

Thoughtful password policies can be an organisation's best hope for protecting against threats. Whilst the use of passwords should not be discarded, an organisation should look at a variety of controls, both technical and procedural, to enhance security, monitor activity, reduce business risk, manage operational impact and achieve regulatory compliance.

The adoption of multiple controls, as well as a formal password policy, will provide visible risk management, reduce risk and the impact of an incident, and inform IT and security strategy now and into the future.

For more information about passwords and identity and access managment, visit www.dxc.technology/security.

About DXC

DXC Technology (NYSE: DXC) is the world's leading independent, end-to-end IT services company, helping clients harness the power of innovation to thrive on change. Created by the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise, DXC Technology serves nearly 6,000 private and public sector clients across 70 countries. The company's technology independence, global talent and extensive partner alliance combine to deliver powerful next-generation IT services and solutions. DXC Technology is recognized among the best corporate citizens globally. For more information, visit www.dxc.technology

DXC_CSC-285_ MD_9467a-17. March 2017