Authentication Past and Future

Passwords are a basic way to control access since ancient times, with the term meaning to provide a specific word before passing through a door, checkpoint or other entry barrier. The word should be secret or have limited distribution. If the word becomes widely known or can be easily guessed, its usefulness for controlling access is lost.

Other means of access control used in the distant past were secret handshakes and special rings or pins. These would identify the persons using them as members of a privileged group allowed to enter restricted places. The secret word, handshake or ring was a means of authentication.

The computer world uses modern updates of these authentication methods. Passwords were first used fifty years ago to protect systems and information from unauthorized access. The Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols perform a secret handshake to ensure transactions are safely completed. Hardware keys contain authentication information serve a purpose similar to a nobleman's signet ring.

The first computer password allowed members of a research group to access files from multiple terminals. From that small beginning, the use of passwords for computer security became standard practice.

Soon, unethical people began using passwords that didn't belong to them. Maybe they wanted to access computer resources for unauthorized research, or to poach expensive computer time without paying. These early password thieves set the stage for a profitable underground industry running rampant across the internet, company networks, mobile devices and workstations, databases and cloud services.

80% of data breaches start out with compromised login credentials (Verizon 2019). Akamai cloud servers are attacked with malicious login attempts more than **30 billion** times each year (Hypr 2019). Attacks are getting expensive too. Credential stuffing costs banks **$50 million** each day (Hypr 2019). Ransomware locks entire networks from access until the asking price is paid. On to top of cyber criminal activity, government regulations designed to protect customer personal and financial data can lead to hefty fines. The price of lost customer confidence and opportunity can't be calculated.

Getting Around Passwords

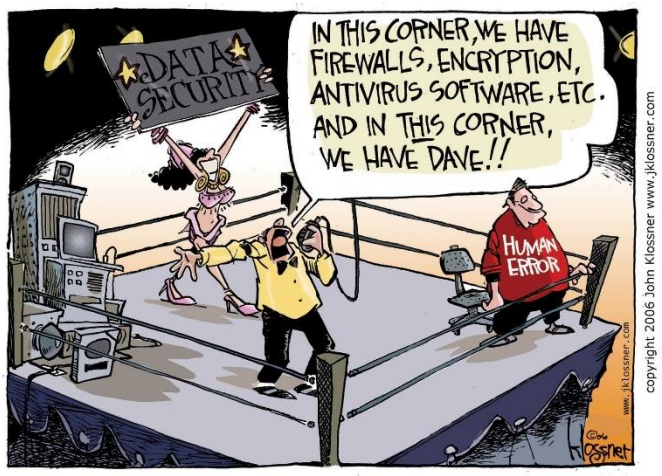
Direct attacks on the network infrastructure of businesses and organizations do happen, but penetrating firewalls and other protections is difficult. More often, hackers focus on employees to access targeted data. Email phishing is the favored attack vector for stealing credentials, eclipsing dictionary and brute force attacks. **90%** of malware infections are introduced through phishing, leading to **72%** of successful data breaches (ENISA 2019).

Spear phishing, a phishing variation that targets specific individuals, has a success rate of **71%** (Varonis 2019). John Podesta, Hillary Clinton's 2016 campaign manager, was a famous spear phishing victim. He received an email warning that his password was stolen. After checking with IT staff, who said

the message was legit, an assistant emailed a password reset link to Podesta. Unfortunately, he clicked the phishing link left in the email thread instead of the genuine Gmail link. A months-long public airing of highly embarrassing emails between Podesta, his associates, and Clinton campaign officials ensued.

No-Hack Needed

Getting passwords without hacking is an easier route. A recent survey of more than 1000 company employees revealed that **34%** share passwords with work associates. Another **34%** write passwords down, and **one-in-ten** admitted to keeping a password list on their computer (SurveyMonkey.com 2019).



While you may know and trust your cubemate Jane, what happens when she leaves the company, or if several password sharing co-workers go on to greener pastures? At what point is a common password changed to ensure security? If password sharing is necessary, it should be strongly administered but typically isn't in most cases. And if someone stumbles across the password list kept in a desk drawer, nothing can stop that information from leaving the building.

Social engineering is another method for discovering passwords without hacking. Extensive background research is performed on a target individual that includes social media posts, career history and educational information available on websites such as LinkedIn. Facebook is a source for hobby, travel, family member, birthplace, and favorite sports information. The profile developed by the social engineer is then used to launch a spear phishing attack or make attempts to guess passwords.

John Podesta also provides an example of how social engineering works. A false story circulated that he had used P@ssw0rd for his email login. He did use that password on a Windows 8 laptop, but not his email account (Politifact). Mr. Podesta's actual email password was Runner4567 which could be guessed using social engineering because he is known to be an avid jogger.

Hack and Crack

Password cracking is another useful tool for getting unauthorized access to data. Cracking a password is easier than many think for several reasons. First, there is rampant reuse of passwords. A typical employee reuses a password **13 times**, while the average computer user enters the same password on **6** websites or applications (LastPass 2019). If workers aren't reusing a password, they are creating weak ones using common words or with slight changes to previous passwords.

Many companies enforce strong password rules and prohibit reuse. That can lead employees to use a password manager, often violating company policy against storing passwords offsite and under control of a third-party.

By 2020, the number of passwords is expected to reach **300 billion** (Cybersecurity Ventures 2019). Small businesses (1 to 25 employees) average 85 passwords per employee. Larger companies (1000 to 10,000 employees) are in better shape, averaging 25 passwords per employee (LastPass 2019). **65%** of large companies have over 500 users who are never prompted to change their password.

It should not be surprising that a lot of the same passwords exist in a pool of 300 billion. Hackers use software to find matches in lists of compromised passwords and lists of the most popular passwords. **91%** of all user passwords appear on the top 1000 list (Passwordrandom.com). The target's email address is used to search lists of compromised passwords, and if they reused their password on multiple websites, a match can be found. Most people don't check to see if their email or password are on these lists.

Top Ten 8-Character Passwords

10	Computer
9	Starwars
8	Sunshine
7	Michelle
6	Trustno1
5	Jennifer
4	Football
3	Baseball
2	12345678

And the most common 8-character password is still …

1 Password

Malware is another method for stealing login credentials. More than **92%** of malware is delivered through email (Verizon 2019). Once introduced, malware can compromise password security on a single workstation, or spread throughout a network. Keylogger malware records keystrokes entered for the workstation login, company network access, internal applications, and websites. The malware sends the logged keystrokes to hackers for analysis.

A software-based keylogger uses smartphone features to reveal a personal identification number (PIN). An example is PINLogger which uses the accelerometer included on most new smartphones. By analyzing motions that phones make during login, the software guesses an entered PIN with **70%** accuracy. There are some caveats for this technology. The website containing the spying application must be open during login, or installed in a standalone phone app. Another challenge is that improving on the initial accuracy requires a neural network and significant software training (Springer.com).

Improving on Passwords

Static passwords are now considered to be hardly any protection at all. In recent years, a succession of new login strategies was introduced to strengthen authentication. While each strategy improved security of the authentication process, they also have flaws that can be exploited.

Two-Factor Authentication (2FA)

2FA is like using a password and a secret handshake. This method was introduced to secure logins for banking, email accounts, and other sensitive transactions. The first factor for 2FA, the password, is subject to the vulnerabilities described above. The second factor's disadvantages depend on the implementation.

Hard tokens are vulnerable to keylogger malware and Man-in-the-Middle (MitM) attacks. Plus, the physical token can be shared with others increasing risk of unauthorized use. There is a small amount of friction in the user experience for hard tokens.

Smart cards improved second factor security by using public key cryptography to perform an encrypted handshake process. This makes a keylogger or MitM attack ineffective. There are some weaknesses inherent with public/private key authentication protocols. And, like the hard token, a smart card can be shared and has the same friction aspect for users.

SMS 2FA replaces the token or card with a smartphone to perform the second factor. The user enters a password (preferably a strong one), then the website or service sends an out-of-band text or email containing a verification code. If the requesting party replies with the correct code, they are authenticated and allowed access.

Unfortunately, SMS 2FA is exposed to several attack vectors. First, smartphone hacking software is available that allows remote monitoring and access to phone functions. SIM swapping is another common method for taking over a smartphone. Malware is become more prevalent on smartphones, with Modliska as an example, which has automated one-time password (OTP) stealing functions. The NIST stopped recommending 2FA in 2016, but it is still in common use. Some cybersecurity experts are predicting that 2FA will be beaten in 2019 (Secrutiny.com).

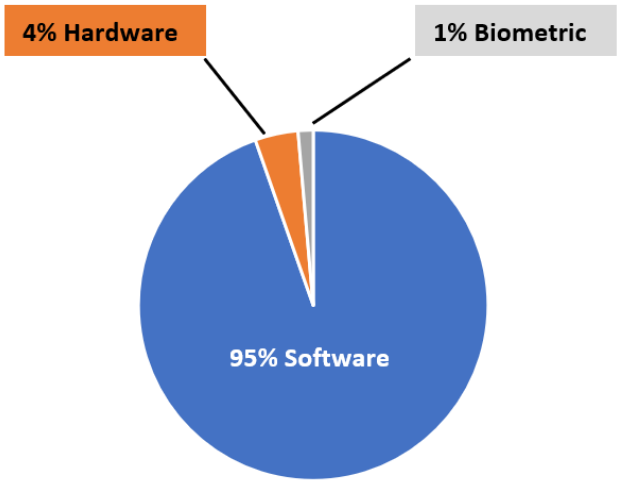
Multi-Factor Authentication (MFA)

MFA relies on the principle that authentication involves something the user knows, something the user has, and something the user is. This translates to a password or PIN, possession of a smartphone and/or

hardware device such as a fob or USB key, and a biometric identifier like a fingerprint scan or location as determined by GPS or IP address.

The PIN is considered less vulnerable than sending a login password to match because that verification step occurs on the phone. The smartphone acts as a soft token for MFA, but subject to the same phone exploits described above. In addition, MFA can be bypassed through the Internet Message Access Protocol (IMAP).

Globally, **15%** of businesses now require MFA by policy, with adoption estimated at **28%** in the US (LastPass 2019). Adoption of MFA by consumer-facing applications is lagging because of cart abandonment concerns (Hypr 2019).



MFA Type Used by Businesses

Going Passwordless

MFA improves authentication security, but users and e-commerce customers prefer the login process to be quick with fewer steps. Tech industry companies formed the Fast Identity Online (FIDO) Alliance in 2013 to create standards for streamlining the process. The alliance developed two specifications: Universal Two-Factor (U2F) and Universal Authentication Framework (UAF).

U2F replaces the second authentication factor in 2FA. User name and password entry is required as the first factor, with a USB key, fob or other hardware device handling the challenge/response with the authenticator. After entering the user name and password, the second factor is validated by inserting the key into a USB port or tapping the fob on a mobile device.

UAF eliminates the user name and password factor for a passwordless authentication experience. A short PIN number entry, or biometric such as a fingerprint scan, is used in place of a password. Authentication of the device is accomplished with the FIDO server challenge/response protocol. The response is signed with the device's private key which the server validates using the corresponding public key.

The FIDO protocols are compatible with Federated Identity Management (FIM) frameworks such as OpenID and SAML, as well as the OAuth web protocol. When the FIDO-based authentication is successful, a single sign-on (SSO) can be initiated with federated websites, web services, and web applications.

Passwordless authentication removes the friction related to 2FA/MFA and greatly reducess common attack vectors. Attacks on weak passwords using social engineering and compromised user name/password lists are not possible. No passwords are sent to a server for matching because initial authentication is performed on the device or workstation. Biometric information is similarly protected

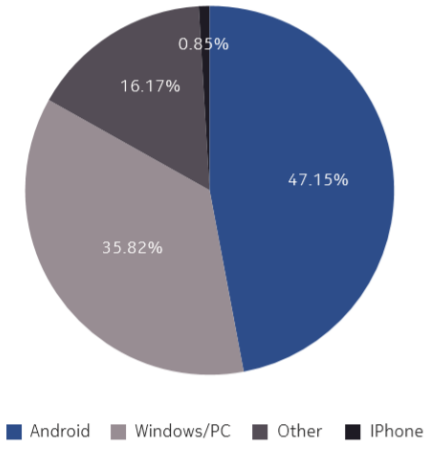
by authenticating the user on the device. Phishing is more difficult because suspect emails are blocked if authentication by the FIDO server fails.

Still No Magic Bullets

Passwordless authentication has some inherent vulnerabilities. While the user experience is mostly effortless, there are many moving parts doing the work. The most vulnerable element is the hardware, followed by public key cryptography and other external operations.

The hardware required for the authentication processes includes a smartphone or workstation, a USB key or fob, and commonly requires two of those devices. Bring your own device, or BYOD, describes the practice of using personal smartphones for authentication.

A stolen smartphone isn't likely to cause a security breach, especially when a biometric factor is used to access the device. The bigger threat from BYOD is malware infection. The **50%** increase in smartphones projected between 2016 and 2020 will make them the largest potential attack vector (IHS 2019). When personal smartphones are used for authentication, security policies should be in place to address the potential threat of mobile malware.



A USB key or fob can also be lost, stolen or simply left at home. If stolen or lost, some devices have a built-in fingerprint scanner to make them useful only to the registered owner. One provider suggests having a second key available. The authentication server can also be unavailable, requiring an alternate process to be used.

Some authentication devices use a PIN entry as part of the process. While a PIN is a shorter version of a password, using a character set of 0 – 9, it's thought to be secure because validation occurs within the device. However, a brute force attack on a short PIN sequence is possible on a stolen device. A user also might choose an easy to remember PIN, like a family birthdate or street address, making it vulnerable to social engineering.

As discussed earlier, the PINlogger malware can use a smartphone's built-in accelerometer to guess password and PIN entries. PINlogger accesses smartphones when connected to an infected website. Other mobile malware is often introduced when users download games and apps outside of the provider's official store. A small percentage of mobile apps installed from official stores may be infected with malware.

Public/private key exchange is used by most passwordless schemes use to authenticate a device. The device uses its secret key to request a connection. The authenticating platform uses the device's public key to verify the request.

Public key cryptography is typically described as strong, but there are well-known weaknesses. The certificates underpinning public/private keys can be forged, stolen, or expired. If a private key is

compromised, it can be used to authenticate another device for fraudulent transactions. Public key cryptography is thought to be threatened by quantum computers that can factor large prime numbers. While quantum computers are expected to be available within six to eight years, recent demonstrations and development efforts by state actors, indicate a shortening of the timeline.

External functions required for the authentication processes include initial device registration, server look-back, and FIDO challenge/response validation. In most cases, the processes are managed by third parties such as the device's manufacturer or service provider, a registration/certificate authority, or a website host.

Devices must go through a one-time registration process linking them to a specific user. A certificate and private/public keys may be installed on the device to be used for challenge/response protocol. Most of this process will be done by an employer or the device's service provider with minimal user input. Trust in the device manufacturer or registration authority is necessary.

Authenticating devices use a server look-back function, accessing lists to determine if an email or incoming data is from an authorized server. These lists can be outdated or inaccurate, leading to a false assurance of validity.

The spread of mobile malware, public/private key exchange, and the external operations required for authentication present attractive attack surfaces for hackers to exploit.

End of Road for Passwords?

Passwords are falling out of favor mostly due to human factors. Each successful tactic to expose passwords was met with an effort to make the passwords longer and more complex to resist the latest attack mode. This created a losing proposition for users who must compose and remember the passwords. So, they choose easy to remember passwords, reuse or slightly alter passwords, and write passwords down.

Password managers came into use as the number and complexity of passwords overtaxed user patience and memorization skills. They are widely used to ensure strong passwords and assist users who are juggling multiple passwords. The downside to password managers is that businesses lose direct control when passwords are managed and stored by a third party.

The next security escalation added authentication steps to foil hackers. When 2FA exhibited shortcomings, MFA was introduced. The extra complication creates more friction for the user who still must compose a unique password every three months, or even more frequently.

In addition to the human factor, passwords have a statistical challenge. When the number of passwords is well into the billions, uniqueness becomes hard to come by. And as the power of computers increases, finding reused and compromised passwords is more efficient.

Cracking passwords is still a significant investment in time and resources, so hackers are getting better results by using various forms of phishing. **90%** of malware infections result from successful phishing (ENISA 2019).

New authentication schemes are starting to take passwords out of the mix, providing many benefits given the threat environment and human resistance to change and chores. Some of the new processes require entry of PIN to get access; proving that the more things change, the more they stay the same.

SUBROSA, In Living Color

Secure Channel's patented SUBROSA passwords can be used with any authentication protocol, just like a password composed with keyboard characters. The key difference is that SUBROSA creates passwords from tile patterns users choose in high definition images. Since they are image-based, the tile patterns are easier to remember than keyboard-based passwords created with complicated rules.

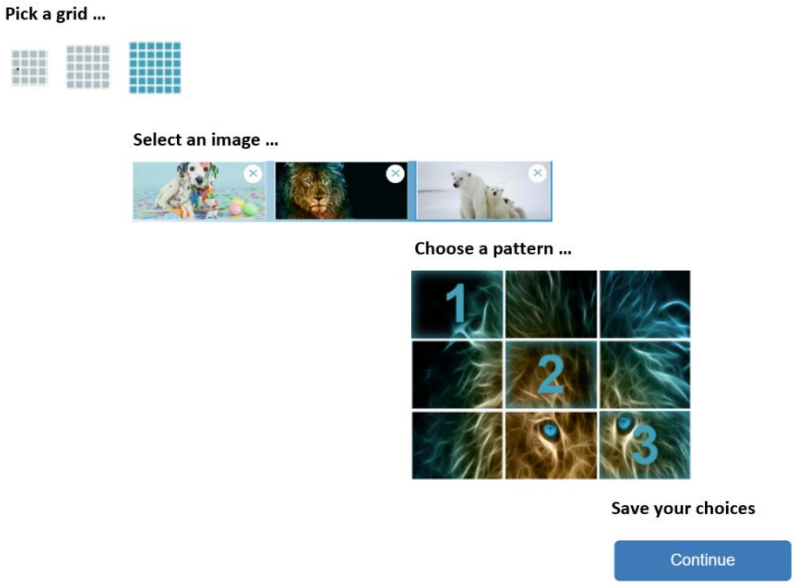
SUBROSA renders the tile patterns into a binary string of 65,000+ characters. The string is encrypted, cryptographically hashed, and stored as a data record in Secure Channels' cloud-based SCIFCOM portal.

SUBROSA passwords are exponentially stronger, block social engineering, and minimize threats like phishing, while making an increasingly difficult task into a more pleasant user experience. Tapping into positive human behaviors to achieve a successful outcome is preferable to causing resistance.

SUBROSA has many advantages over traditional passwords. First, the user only knows the tile pattern, not the password it generates. Only the user-selected images are stored on a device, website or application server. The entire image library and the tile pattern's hash value is stored on the SCIFCOM server. The hash value is calculated each time the user to authenticates.

Users can customize SUBROSA passwords in several ways. They can pick a bigger grid for more tiles, select tiles on more images, and choose more tiles on an image. Users can personalize their login by uploading their own images. This creates a stronger password and a fun user experience as they choose tile patterns from images of their children, pets, favorite vacation spots, sports teams, and hobbies.

SUBROSA password creation is beautifully simple.



No keyboard is necessary. Mobile and workstation touch-screens or mouse-clicks are the authentication interface.

SCIFCOM Portal

SUBROSA is integrated with Secure Channels' cloud-based SCIFCOM portal. The SUBROSA functions on the portal include initial setup, image repository, password data record storage, hash value calculation, and authentication pass or fail result. Interactions with the portal are uniform, but SUBROSA implementation is specific to the platform use case. Platforms include websites, devices, web services, and cloud-based or locally-installed software applications.

For example, a website login is implemented using SUBROSA-generated API code. Alternately, the login for a device platform is implemented with code from the SUBROSA Software Development Kit (SDK). Both platforms follow the same protocol to request authentication and provide image/tile selections for processing.

Performing the SUBROSA authentication process through the global network of SCIFCOM servers has several advantages.

Breach Protection

In many cases, login credentials are stored on a server associated with the platform the user wants to access. For example, when a user logs into a bank's website, an authentication server is queried to validate the submitted credentials. Password records are a common target of attackers. Usernames and passwords obtained through a system breach can be sold and then used in large-scale credential stuffing attacks.

SUBROSA passwords, the user-selected tile patterns, are not stored on the SCIFCOM server, so an attack can't yield any credential-related information. The password hash values stored on the SCIFCOM server can't be reversed to reveal information to hackers.

Blind Transactions

The secret key associated with the user's SCIFCOM account is the only identifier used to locate the stored data record for comparison to the calculated hash value. The authentication pass/fail notification is returned to the initiating platform which allows or disallows the login to proceed.

Redundant

SCIFCOM servers distributed across the globe are randomly-selected to process authentication requests. In the event of a Denial of Service (DoS) attack, multiple servers are available to process authentication requests.

Economical

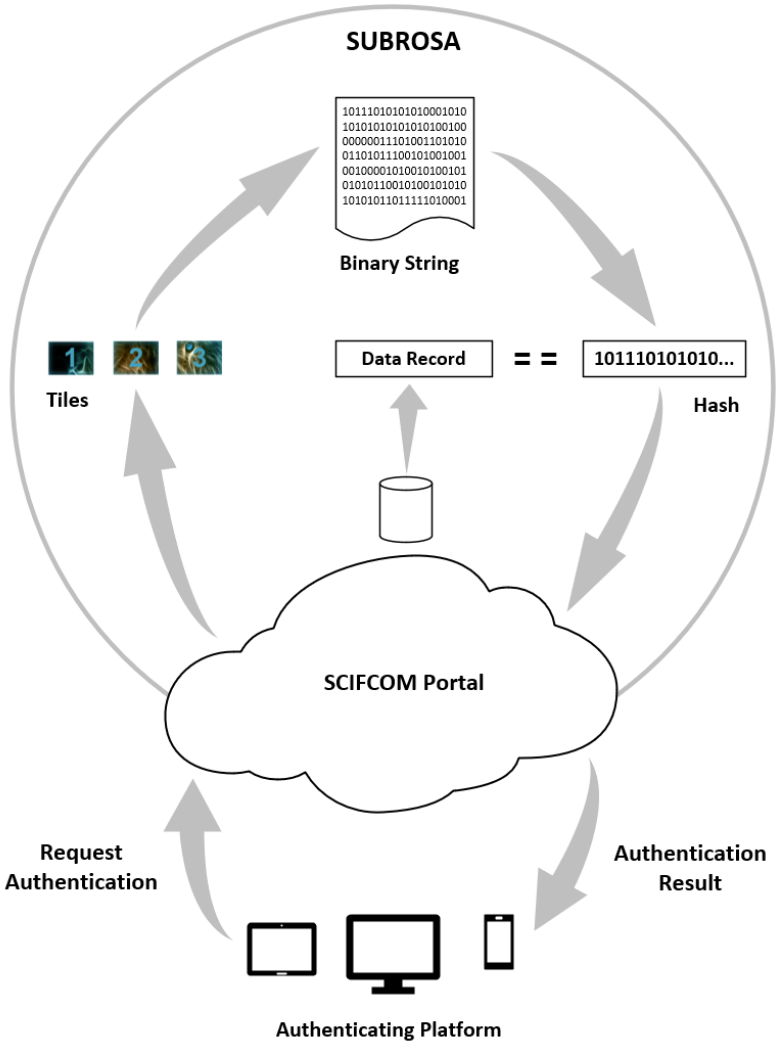
There is no need to contract with a third-party to store and retrieve credentials. A flat rate is charged for each authentication transaction performed through the SCIFCOM portal.

Safe

All data records, images and configuration settings residing on the SCIFCOM portal are encrypted.

Authentication Process

Signing in to your device, website or service is simple too. Users initiate authentication by selecting their tile patterns for each image. The tile selections are processed into a long binary string, encrypted and hashed. SUBROSA compares the calculated hash value against the hash stored in the user's data record. The SCIFCOM portal provides the result, pass or fail, to the requesting platform.



SUBROSA Authentication Process

The SUBROSA Solution

SUBROSA eliminates the well-known weaknesses of traditional passwords and delivers significant advantages for authentication. Even though SUBROSA is used just like any other password, there is no shared secret in the traditional sense. The user only knows their secret tile patterns, not the binary string SUBROSA creates, or the resulting hash value. All authentication steps are performed on the secure SCIFCOM server.

SUBROSA takes away the user's reasons for using password shortcuts and avoids common attacks.

No weak passwords

Constantly composing strong passwords is a chore, causing users to take slightly alter and existing password or reuse the same password for multiple logins. Even when strong rules are applied, the vast number of passwords in circulation risks duplication with an existing password.

SUBROSA password creation liberates users from the keyboard, placing them in a visual realm to perform the simple task of picking tile patterns. The SUBROSA password is derived from the user's tile patterns, then hashed. Duplicate hash values (called collisions) are mathematically unlikely.

No password attacks

Hackers employ many attack techniques such as dictionary and other searches, social engineering and phishing. Visual-based SUBROSA passwords defeat these usually effective attacks.

Dictionary attacks and searches of compromised password lists are used against traditional passwords. Login credentials exposed in a data breach are used for credential stuffing attacks because the same credentials are often used on other sites.

The binary string rendered by SUBROSA is not human readable and unknown to the user. There are no dictionary words or compromised passwords to search.

Social engineering is a successful strategy for guessing passwords or crafting an effective spear phishing email. SUBROSA is immune to social engineering because it can't help an attacker to guess a user's tile pattern selections.

Phishing for login credentials doesn't work with SUBROSA passwords because the target only knows the tile patterns, not the password

More Advantages

The visual nature of SUBROSA passwords offers advantages to enhance any authentication strategy.

Users add more images, choose more tiles, or select a different grid to make a SUBROSA password stronger. The only way to make a traditional password stronger is to make it longer and include special characters, making it much more difficult to remember.

SUBROSA authentication takes place on the SCIFCOM secure portal, not on the user's device. Configuration settings, the image library and data records are stored on the secure server and can't be compromised from the user's device.

Keylogger malware is ineffective because no keystrokes are used to enter a SUBROSA password. The same goes for malware that uses a phone's accelerometer to guess password characters.

Even if a device is cloned, taken over with a SIM swap, or loaded with hacking software, the SUBROSA password can't be compromised because the tile patterns are in the user's head, not in the device.

Conclusion

SUBROSA flips every good reason given for abandoning passwords. Image-based passwords created with SUBROSA appeal to positive human behaviors and make keyboard-based password attacks useless.

The simple password creation process ends the time-consuming task of composing passwords. Making up passwords becomes a pleasant and intuitive experience. Shortcuts that cause weak keyboard-based passwords can't be used. Even with no strict rules, every SUBROSA password is uniformly strong.

SUBROSA passwords erase a decade of hacker progress. Today's most successful attacks are ineffective: no dictionary searches, no credential stuffing, no social engineering, no phishing for credentials, and no keyloggers. Exploits against authentication devices are also largely short-circuited. Smartphone hacking software, cloning and SIM swapping can't expose a SUBROSA password because it's not stored on the device.

SUBROSA fits perfectly into the mobile experience. Entering password characters on a tiny smartphone keypad is unnecessary for SUBROSA passwords. A touch screen or point-and-click mouse is the password entry interface. No more dealing with fat-finger mistakes and back-spacing corrections.

SUBROSA flips every good reason given for abandoning passwords. Just as the usefulness of keyboard-based passwords fades, SUBROSA image-based passwords strengthen authentication processes.

Passwords aren't dead, but keyboard-based passwords are. SUBROSA ends keyboard-based passwords and begins an image-based authentication paradigm. Users get a beautifully simple password creation process while attacks developed over decades are made obsolete.