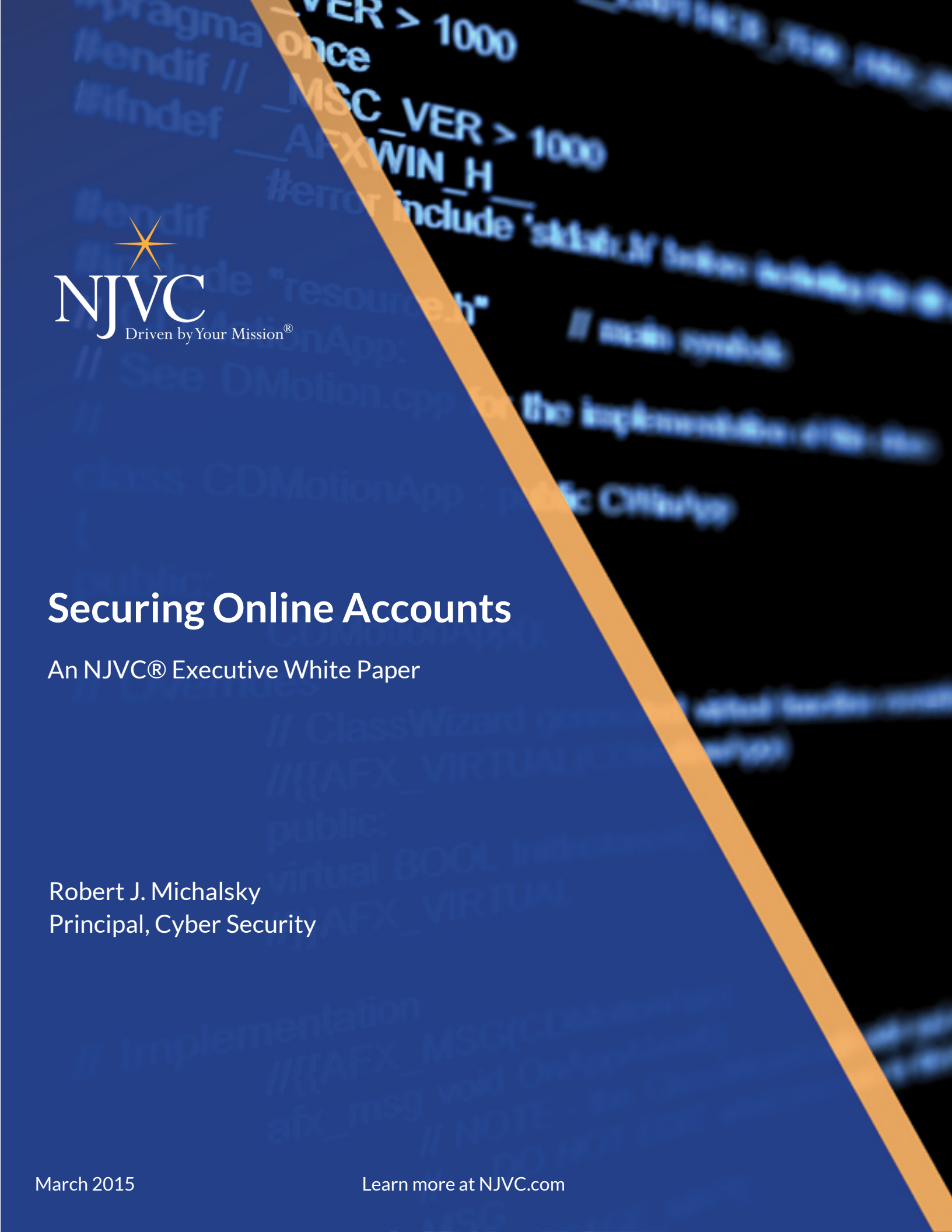

NJVC
Driven by Your Mission®

Securing Online Accounts

An NJVC® Executive White Paper

Robert J. Michalsky
Principal, Cyber Security

March 2015

Learn more at NJVC.com

Securing Online Accounts

Online accounts of all types continue to proliferate. There are accounts to order goods and services online. There are accounts needed to read online subscriptions. There are accounts to upload and download personal information including items such as photos.

Regardless of the purpose of the account, however, all types include the need for both authentication and authorization.

Authentication is the process of proving who you say you are to a system. Authorization is the process of the system granting you the rights to use that system. Taken together, they provide access to online accounts and in theory only allow the authorized user to access their account.

Identifying users via an account ID and password is the most common user authentication and authorization scheme in use today. The password is a string of characters that serves to authenticate the user by making them provide something they know. However, this scheme is also one of the weakest given how poor passwords are often selected, used and managed.

For better or worse, passwords do not appear to be going away any time soon. They continue to exist and proliferate as they balance user convenience with some resemblance of security for a wide range of software applications.

According to most reports, the average consumer has between 25 to 30 online accounts they utilize on a regular basis – all of which require some type of password. It is quite unreasonable to expect each of those to be unique and to follow the various strong password rules implemented at multiple websites. Moreover, often lost in these discussions is that whoever is running the online account for the organization in question bears responsibility to properly store and manage user passwords.

So what can be done?

Let's try to look behind the monitor and uncover what is going on in a world full of online accounts featuring single-factor authentication schemes centered on user names and account passwords.

- What are the best password protection mechanisms?
- What are effective techniques a user can implement?
- What is on the horizon to replace passwords?

These and other questions have a significant impact on whether a specific account will be cracked exposing a user to various illegal credential exploitation activities such as Identity Theft.

Background

In recent years, data breaches have become a common and recurring news story. Seemingly no day goes by without mention of yet another organization suffering some type of network breach and data disclosure. To an average user, this may lead to an incredible amount of news fatigue on the topic and a subsequent lack of interest in crafting strong passwords. Data breaches in the news typically involve a large collection of user data (passwords, account credentials, credit card numbers or other protected information). All industries appear to have been targets and with the total quantity of breached records totaling in the millions – this has only increased the amount of user apathy.

Federal regulations in certain industries reinforce this sense of breach fatigue even further by requiring some type of public disclosure such as a public web site posting or press release. For instance in healthcare, HHS regulations on protected health information require data breaches of 500 records and above to be publicly reported.

Further exacerbating the situation is that users typically feel no direct impact. Credit or debit card number disclosures for large breaches lead to a reissuance of new numbers and life goes on. Certainly identity theft cases are on the rise, but data thieves are primarily interested in monetizing their stolen assets, not doing personal reputation damage.

After large breaches, companies are quick to offer some sort of free identity protection service as a means to perhaps protect the individual who had their credentials stolen. The primary purpose however is to protect their business reputation and minimize liability issues.

The news media is often quick to criticize users , in particular after researchers get their hands on a stolen set of unencrypted password data and report the most common passwords in use are ‘123456’ or ‘password’.

Yet, factors unknown to users can have a very significant impact on the likelihood of an account being compromised. In particular, how are the account credentials stored? As you might imagine, expending effort on the storage can greatly enhance the security profile of the data.

This topic is often not mentioned because organizations do not want to be embarrassed by revealing how poorly they may have implemented their password protection mechanisms or other data security controls.

Let's pry this door open a bit and take a look inside.

Research

Passwords are an obvious and important factor in IT and the digital landscape and yet relatively little active research has been performed. In large part, this is because of the difficult nature of gathering real operational data across a number of environments. Organizations are not interested in sharing any of their operational data limiting the ability of researchers to perform analysis on realistic data.

Microsoft however, has performed a number of studies and with their worldwide installed product base, has provided some of the best insights to this murky area. A paper by Dinei Florencio and Cormac Herley (A Large-Scale Study of Web Password Habits) is particularly compelling because the authors got approved access to over a half million accounts over a three month time period through a Windows Live Toolbar component. In short, they had access to real operational data.

Why do users choose weak passwords? Their study revealed the average user has 6.5 passwords that they use for each of 3.9 different sites yielding each user having over 25 total accounts. In an average day, a user types a password 8 times.

Further, their analysis reveals just how bad the situation is. An 'overwhelming majority' of passwords use lower case letters only (no Upper case, digits or special characters). This simple fact is why so many sites now explicitly ***force*** users to include an upper case, numerical digit and/or special character. Including just one of those symbols goes a long way to improve the strength of any given password.

Interestingly, lowercase values predominate in all length passwords. From their data, this holds in all passwords from character length 8 through 16. As obnoxious as it may at first seem to an end user, the simple practice of combining lower and upper case and digits and special characters in some blend *is effective*.

Still, their results also found that for accounts with more consequence (e.g., financial services), a higher bitstrength of 51.4 was noted as opposed to a value of 38.9 for lower value sites such as those protecting subscription access to news sites. As an overall

average, users ***do*** make some effort to better protect their more valuable accounts. Unfortunately, their data also reveals that less than 2% of all passwords are considered 'strong' via a combination of lower and upper case and digits and special characters.

In summary, depending on users to create and manage strong passwords across all their online accounts is simply not going to happen. But there is a lot more to the story than what users select and use for their passwords. Something that receives far less attention is how those password files are stored and maintained.

Password management

Passwords themselves may be weak, but if they are properly managed, updated and kept secret, they can still provide an effective account protection mechanism. Proper storage can greatly help prevent theft and account compromise through collecting and exploiting data from system log files and backups. In fact, strong password storage designs can strengthen resistance to a variety of attacks - restricting system access even after account credentials have been stolen.

In general, password storage mechanisms fall into four categories: (in increasing strength order)

- Cleartext
- Encryption
- Hashed
- Hashed with salt values

Cleartext means storing the credentials without any protections whatsoever. The file is visible and interpretable directly to anyone reading the password file. File access protections may still be in place, but once the file has been located, the attacker has full file access available. Finding the password file means ***all*** accounts have been compromised. This is obviously not a reasonable approach.

Encryption is the process of transforming data to keep it secret from others. The intent however, is to be able to reverse the algorithm making this method less than optimal for storing passwords. It is a useful technique for storing credit card numbers, where the data can be stored in an encrypted form, and with the key, able to be reconstructed as the original data. This is a less than ideal method for storing password however, because should the encryption key be compromised, an attacker is able to decrypt each and every account.

Hashing takes arbitrary input and produces a fixed-length string. The same original data always produces the same hashed value. It is a one-way function given the fact that the computed data cannot be reversed back to its original cleartext form. As such, this function is ideal for storing passwords because the original cleartext is not known by the system and yet the hashed input value can be compared to the original hashed password value to determine if the user has input the correct password. Hashes have no key.

As strong as hashing is, it is still susceptible to an attacker who is able to take a dictionary set of entries and run them all through the hash function and test each result. Depending on the hashed value length, it may also be susceptible to a brute force technique. To counter that and increase the strength still further, salt values are used.

A salt value is a fixed length random data value that gets added to the credentialed data and greatly increases the entropy of the output function. This makes the technique valuable because it does not require any additional effort on the part of the user and yet thwarts both pre-computed dictionary lookup attacks as well as making time based brute force attacks computationally infeasible. In essence, it adds in a sufficient amount of randomness. Iterating over the hash multiple times (called key stretching) offers the absolute best protection, even against brute force attacks since the hash and the salt values are used as inputs during each iteration.

Another utilization of hashing is to preserve data integrity. A one-way hash is a function that takes a variable length string and a message and produces a fixed length value called a hash value. This is a method of fingerprinting a message – making sure it was not tampered with during transmission. Strong hash functions do not produce the same hash value for two or more different messages.

Different Operating Systems support different password storage mechanisms. For instance, passwords in Linux and Unix systems are stored in a file containing the hashed value of all the passwords. To further enhance security, the salt (or random number) is thrown into the mix to add more complexity. The more randomness introduced into the process, the harder it is for adversaries to reverse engineer the process and uncover the original password.

A salt - being a fixed length cryptographically strong random value - is appended to the account credential data and provides increased protection while not increasing credential complexity and imposing more burdens on users. This makes pre-computed look up attacks infeasible while minimizing requiring users to generate long length strong passwords.

Guessing versus Cracking

There are two distinct paths to having passwords broken. It is important to be aware of this when evaluating each Use Case.

Guessing is having someone or some type of software make repeated attempts by trying a value directly against a software application. A human can make repeated manual attempts at a login screen, but more likely software is used to automate the process, increase the quantity of attempts and increase the likelihood of success. Lists exist of common and popular passwords and these can be tried in sequence. This is sometimes referred to as '***online***' since it is conducted against live web applications.

Cracking is a completely different situation. Here, an attacker has already compromised some portion of an IT system and has obtained the raw hashes of the password values. An attacker generates test passwords, hashes them and then compares that result to the uncovered stored value. Cracking is exponentially faster than guessing. This is sometimes referred to as '***offline***' because the attack can be conducted using dedicated hardware and software with no live application connection required.

While online attacks are common and easy to carry out, they have many built in limitations. Applications can limit the amount of incorrect passwords able to be entered. Time limits can be placed on password entry, preventing automated software approaches from being used. Accounts can be locked after any policy violations. While this directly impacts the user, it does alert them to the attack and they can notify the organization holding the credentials.

A determined adversary conducting an online attack should be noticed by IT security staff or their automated mechanisms. Either account alerts or activity monitors should be able to convey an attack is being conducted. Rules such as automatically blocking source IP addresses can be put into place. As a result, online attacks do not require overly strong passwords be in place to resist an attack. In fact, the previously mentioned Microsoft paper proposes a number of only one million as the number of guesses an online password attack must withstand to be considered 'strong'.

Offline attacks are a completely different case. All the computing resources available to an attacker can be leveraged and thrown at the stolen password file. The more compute horsepower available, the higher number of password crack attempts per unit time can be generated. As a result, the Microsoft authors estimate an offline attack needs to withstand 100 trillion attacks to be considered 'strong'.

For an attacker, obtaining the password file for an organization is a high priority, and many 'low and slow' advanced persistent threats are conducted exactly for that purpose, finding a network infiltration point and then pivoting across network domains looking for the valuable password file.

Since obtaining password hash tables typically requires administrator access, why would an attacker bother with all the effort to crack a password file? To determine the values that might prove useful when targeted against other accounts. It is because of this cross – account issue that a recommendation to not reuse passwords across accounts usually shows on a password tip list.

In addition, there is a class of attack called 'Pass The Hash' where an attacker who has compromised a network to obtain user password hash values uses that data to authenticate into other remote services exploiting a weakness in the authentication protocol often used that do not require salt values to be used.

Passwords versus Passphrases

What can be done to make passwords more resistant to attack?

While a password is typically defined as a series of random characters of a specified word length, a passphrase is generally a series of words that may or may not include spaces. The token utilized changes to words instead of characters. This 'chunking' of data has a definite role in analyzing the difficulty of uncovering the value. In addition, because of the ability of humans to remember words easier than random characters, passphrases tend to be longer than passwords. That length however, does not necessarily imply greater protection.

Since users can remember passphrases that are longer than passwords, it is generally assumed passphrases are more secure. This breaks down however when we uncover that attackers use 'dictionaries' which are lists of common words.

The average length of an English word is five characters. Studies report the median pass phrase only contains 4 words. Having passphrases longer than 4 words improves their security but means users are then forced to remember over 20 characters. At some point typing proficiency also enters the picture (particularly on mobile devices) and the inherent difficulty factor means from a usability standpoint, users will not comply unless forced. (and if forced – may opt for a different service).

Password length has a direct correlation to difficulty of being broken. 9 characters are more secure than 8 which is more secure than 7 and so on because more computations must be performed against longer word lengths.

Data Breaches

As mentioned, data breaches are a common news item. At times hackers have posted their stolen password files and researchers have been able to study what passwords were in use.

Much media attention targets users and their preferences for using quick, simple and easy to remember passwords. Many writers opine "if only users all used strong passwords…", implying this action alone will solve the problem. That is not true, however. As we noted, password strength is but one factor in surviving the attack of a determined adversary.

Given the critical and growing role of using passwords to guard key online data, hackers are maturing the sophistication and tenacity of methods to harvest this data. This is leading to the wide proliferation of data breaches.

Large breaches are often the results of attackers getting more sophisticated. Instead of targeting a series of individual accounts, attackers are looking to penetrate organization networks (where password files are kept) and simply steal the entire password hash file. Having that data available then supports offline attacks where they can utilize large amounts of compute power.

Successful phishing attacks harvest account credentials through impersonating a real web site or application and getting a user to willingly reveal their account credentials. This is particularly pernicious because no strong password can overcome the user being duped to simply give it away.

In a similar manner, a category of malware called 'key loggers' may lie in wait on a PC to surreptitiously gather user credentials as they are typed in to a web form. Here, a user is not misled into going to a bogus site or responding to a fraudulent online inquiry. Instead, the malware evaluates the URL of a target web site and simply waits for account credential fields to show up on a web form. It logs the keystrokes and communicates through a backchannel to a site where the credentials are sent.

Hence, in cases such as these, strong passwords will have in essence ***no effect***.

Account categorization

Not all user accounts are created equal. Certainly one of the key factors in password 'fatigue' is the fact that often each and every account considers itself worthy of a 'strong' password and will force users to create one – (reportedly for their own benefit) – but actually because the IT staff which may not have extended sufficient effort on their end to secure the critical password file.

For those interested in more details, Dinei Florencio and Cormac Herley of Microsoft Research along with Paul C. van Oorschot from the Carleton University in Ottawa Canada have built a formal account categorization model which uses four levels ranging from Level Zero "the user doesn't care" up to Level 3 "High consequence". An additional "Ultra-sensitive" category is reserved for business transactions where an account compromise can cause irreversible damage.

The effort expended to maintain protection levels should be commensurate with the value of the data being guarded. Of course data value is a matter of perspective, and users very much resist having to create strong passwords in situations where they feel the effort is not worth it. System administrators would be well served to keep this in mind when creating security policies.

Determining if your account has been compromised

Besides the generic 'change your password' message after a new data breach has been reported, how can one tell if their account has indeed been compromised? One of the best methods is this site built by Troy Hunt a cyber engineer with Microsoft[1].

This site allows one to enter their email address and it will search through a massive database which Troy has aggregated which includes all the data from over a dozen of the most recent and largest data breach events.

In addition, Troy has uncovered that from 16% to 22% of the emails in the breach list are seen in one or more account listings. Why should a person no reuse their credentials across accounts? For this very reason – a compromise in one account can give an attacker direct access to your other accounts. For instance, given the size of the Adobe breach in October 2013 (153 million accounts exposed), Facebook even went so far as to match up the exposed credentials and suggest to their impacted users they change their password.

[1] https://haveibeenpwned.com/

Since any tool can be used for both good and evil, it is unfortunate that attackers have access to this capability, but for the average consumer, it gives an explicit signal that you should take the generic warning seriously and indeed change your password. Many of us may have created an account long ago forgotten – that has now been compromised – and can lead to other account compromises if credentials are being reused across sites.

It is also important to note that Troy does not maintain a database of the passwords. The value he is interested in conveying is simply if your account credentials have been breached and that you should change your password.

As of February 2015, his site has 37 separate websites listed containing over 175 million accounts. As new public breaches are reported, he integrates that into the treasure trove and life goes on.

Password Managers

What else can be done to implement stronger passwords without injecting users with mass quantities of new memory cells in their brains?

One approach to implementing stronger passwords across a wide number of accounts is to use password manager software. This class of software stores and organizes passwords. The products can easily handle however many accounts an individual uses and replaces the burden of having to remember dozens of strong passwords with the burden of only having to remember one single strong password. The 'master' password provides access to the database of passwords which can be stored in an encrypted fashion. The password database can be stored locally or on a cloud structure.

In addition, these products typically provide some protections against malware such as key loggers or other memory scraping software. For those so inclined, many products also have random password generators built in so strong passwords can be used for all accounts without the user having to generate or remember any of the passwords.

It is beyond the scope of this paper to dive deeper into this topic and the details of how this software works, but suffice to say, online evaluations of this category of software product appear regularly. Two recent articles of note from PC Magazine[2] and CNET[3] are

[2] http://www.pcmag.com/article2/0,2817,2407168,00.asp

[3] http://www.cnet.com/news/best-password-managers/

located below. The best part is that they regularly update posts such as these when new product capabilities warrant a technical refresh.

Cost is not an issue as many of these products are free since they are based on open source code which has been refined by zealous programmers contributing to the greater good. Advanced features require a subscription cost, but vendors add in capabilities such as the latest breach alerts or secure cloud backup storage to justify the cost.

Emerging Technologies

While no single technology has emerged to replace the password, technological innovations continue to present themselves as a potential solution to enhance the protection of online accounts. Next generation passwords are available today, but typically lack sufficient market presence to make them truly usable across a wide range of systems, devices and applications.

Are other methods available? Hardware-based authentication is useful in controlled corporate networks, but cost and deployment complexity are limiting factors for general purpose usage. This may change over time. Windows 10, for instance, currently plans to support hardware trusted device establishment, which will enable two factor authentication for a PC, tablet or phone in combination with a PIN or biometric proof. If this proves effective, the controls may move from a corporate IT environment to general purpose usage.

At present however, most consumers simply do not want to have to carry a 2nd factor of authentication (such as a token or a smart card) that would not be usable across all or at least most of their accounts.

Question-response interfaces are widely available but are thought of as too time consuming for general account access. Instead, they are deployed as an additional level of protection when performing certain sensitive account actions (credit card entry, password change etc.) In addition, general purpose questions all too often center on information available in the social media information swamp.

Two factor authentication schemes do strengthen a password but typically require a user to carry something to authenticate their identity. For consumers, one device has emerged that is allowing a coalescence of factors to come together – the smart phone. Using their smart phone along with authentication methods such as one time passwords or PIN codes adds to protection levels on accounts where the password hash file may have been stolen.

For retail transactions, Apple has extended a one way token concept (Apple Pay) – where an encrypted passcode is sent to a mobile device and tapped or swiped to enable the authentication. The token would not be reused - which enhances security. If this is enabled through an application, the process of logging in would be the second authentication method. The tapping is done via Near Field Communications (NFC) which allows devices to communicate with each other without using a radio frequency thus making eavesdropping difficult.

Biometrics

These biologic based factors have existed for years and continue to delight science fiction fans. The idea is to use a fingerprint or iris scan or a palm pattern – something distinctive and associated with your physical self – in order to authenticate. The Apple iPhone 5s introduced these to the world of mobile phones and the technology continues to drive its pricing down. The reason in the past which limited widespread adoption is the high rate of false positives – meaning authentication is accepted when it should not be – which is obviously not the intent.

As combinations of mobile device authentication along with biometric sensors emerge, more stringent two factor authentication schemes become practical and begin to address the widespread usage issue.

Fingerprinting

Probably the most common and well known biometric identification technique, fingerprints have long been used in forensic science and have recently moved into the mobile device world for user authentication. Not only are fingerprints unique to an individual, they are long lasting and difficult to alter, making them effective over time.

Digital tattoo

These are flexible electronic devices worn directly on the skin (similar to a band aid) – and perform authentication via NFC. Taking the concept even further, is the idea of actually injecting a tiny microprocessor directly under the skin.

Password pill

Here users swallow a small 'pill' that can generate a few bits of data. Ingestion of biometric sensors do not have widespread acceptance from typical non-technically oriented users.

Iris or retina scanning

The iris of the eye of each person is similar to fingerprints in its biologic complexity and can be used as a unique identifier. Mathematical pattern recognition algorithms are used to identify an individual. The blood vessels of the eye can also be used since they form unique patterns. Even twins have different retina patterns and can be differentiated.

Voice printing

Here, voice recognition is used for authentication. An individual speaks a passphrase and the voice print is matched against a stored value. The actual phrase is not as important as the voice itself. Thus voice prints are not simply based on a statistical representation of a population, but instead a characterization of an individual voice. As a result, voice prints are similar to fingerprints in their ability to characterize a specific person. They provide 'Go' or 'No Go' user authentication experience.

Voice commands have intrinsic value because they support hands free operations. When combined with voice printing capabilities, they also enhance security in a wide range of authentication situations when accessing and using personal data. Stolen devices are rendered unusable when secured by this technology.

Going still further, these applications can be combined with GPS enabled systems to offer location security on top of the user authentication security, allowing only specified applications to work at particular locations.

Federal Government Role

The concept of replacing passwords and creating a more secure authentication process has been around for years. It was in April 2011 that the "National Strategy for Trusted Identities in Cyberspace" was first released by the White House. This effort is overseen by NIST (National Institute of Standards and Technology) and is continually evaluating new methods that can lead to a 'trusted cyber-ecosystem' without having to rely on passwords.

The intent is to rally public support behind market driven solutions that will be widely adopted and will balance convenience and security to create a useable solution. Complicating this effort is the desire to also incorporate privacy concerns and to make sure personal data such as Electronic Health Records (EHR) can be used to share sensitive data in a secure manner across multiple healthcare providers.

There are four primary guiding principles being put forth:

1. Identity solutions will be voluntary and privacy enhancing

2. Identity solutions will be secure and resilient
3. Identity solutions will be interoperable
4. Identity solutions will be cost effective and easy to use

To support this, various pilot projects have been initiated and funded.

More details can be found at: http://www.nist.gov/nstic/

An obvious complicating factor here is that in a competitive marketplace; companies do not want to collaborate on solutions and will tend to create proprietary systems that may have many inherent advantages, but not received widespread adoption across multiple markets. The hope is that a framework can emerge that can lead to standards that will enable real solutions over time. Interoperability of strong credentials across multiple domains is the ultimate objective.

In support of that, the numerous data breaches reported have served to raise the awareness of the general public to the threats their online accounts face and to be more open to the adoption of new technologies to protect their data.

Industry Alliance - FIDO

Many companies have joined together to address the reluctance of users to embrace anything beyond a single factor authentication scheme such as a password. The FIDO (Fast Identity Online) alliance is a non-profit, industry consortium formed in July 2012 to address this very issue. The goal is to define an open, scalable interoperable set of mechanisms to reduce the reliance of users on passwords.

The intent is to support a full range of authentication technologies and yet retain a device centric model that can be adopted worldwide. These companies envision a future where any website or cloud application can use standard interfaces on a wide range of FIDO enabled devices to provide robust online authentication.

Creating interoperable standards is the key to have new applications and devices be able to participate in a secure online authentication ecosystem. Online service providers can take advantage by setting their own policies about what type of authentication methods they are willing to trust. PIN codes, voice recognition, fingerprint readers and other biometric methods thus become eligible for participation.

FIDO holds out the promise to maintain user convenience while enhancing online security. The alliance continues to add member companies with Google being perhaps the most noteworthy addition. Founding members include Nok Nok Labs, PayPal and Lenovo.

Summary

Passwords are not going away anytime soon. They strike a balance between convenience and security that is hard to replace and has widespread acceptance – in spite of the reported security issues.

While sometimes it seems users are always being blamed for their selection of poor passwords, the proper storage and protection of those password files can overcome some portion of that weakness.

Even though the actual selection of those passwords is entrusted to system users, IT personnel can utilize a wide range of techniques to insure their handling of the critical password files are protected to the highest degree possible.

Even after a data breach has exposed records, administrators can enforce techniques to minimize the impact and lessen the economic worth of the stolen data.

New convenient technologies such as the iPhone fingerprint enable the 'defense in depth' security principle to be enabled, leading to a higher security posture for all users and all data.

About the Author

Robert J. Michalsky has served government and commercial customers for more than 30 years providing a wide range of IT and analytical services. As NJVC Principal, Cyber Security, he quantifies and pursues new business opportunities in cyber security. Mr. Michalsky has spent nearly two decades providing cyber security-related IT engineering and architecture services for classified Intelligence Community customers.

Appendix

Authentication – the process of proving to an IT system that you are who you say you are. Usually done as a combination of knowledge (something you know), ownership (something you have) and personal characteristics (something you are)

Authorization – the process of the IT system granting you specified rights to use that system. For a file this could be read, write, delete etc.

Bitstrength – a measure of the strength of a password in resisting guessing attacks and brute force enumeration techniques. There is math behind the summation, but by way of example, a 9 character password that contains both upper and lower case characters and digits has a bitstrength of 53.6. The average found in the Microsoft half million account study was 40.5, significantly lower.

Cleartext – a password stored in human readable form and visible just as the user input it. Offers no account protection whatsoever should the file be found by an attacker.

Cryptographically Strong – Cryptographic algorithms need to demonstrate their resistance to attack in a public forum. 'Strong' is an inexact term but usually refers to a sufficient degree of randomness and resistance to attacks when evaluated in this manner.

Encryption – the process of changing source data into a different output form for the intent of keeping the data secret from others. One similar physical system is that of a safe deposit box, which also uses a key for access and only allows the owner (or others who have the key) access to the contents of the box.

FIDO (Fast IDentity Online) – A non-profit industry organization establishing a set of interoperable standards that enhance online user authentication. A wide range of authentication methods are being supported enabling third parties to build to a set of standards creating on overall authentication ecosystem.

Hash value – mathematical representation used to store password values and not have them be accessible in cleartext

Hash function – a mathematical algorithm used to perform a one way transformation on a password to obfuscate its value. One physical way to think of this is using food, once raw ingredients are combined and cooked (with bread for example), it is practically impossible to go and reverse the end product into its original ingredients.

Near Field Communication – a two way, short range, wireless communication method often used in contactless payment systems. It is based on older Radio Frequency Identification

(RFID) systems but does **not** use a radio frequency for communication, hence is more secure and resistant to eavesdropping.

Password - a series of random characters of a specified word length. Prime method used for knowledge based authentication.

Passphrase - a series of words that may or may not include spaces and meant to replace a password

Pwned – computer science industry 'slang' for a personal account being 'owned' by a person or remote process taking control of another computer. The original misspelling has stuck and the term is now part of the cyber and IT landscape.

Salt – a fixed length cryptographically strong random value

Two factor authentication – an authentication process that strengthens a password by requiring a user to carry something to authenticate their identity. The device could be a mobile phone or a token of some sort such as a dedicated key fob.