

The World Will Need to Protect 300 Billion Passwords By 2020

By Steve Morgan, Editor-In-Chief Cybersecurity Ventures & Joseph Carson, CISSP, CSPO, CSP, Thycotic

As the total universe of passwords will likely grow from approximately 90 billion today to 300 billion by 2020, organizations across the world face a massively growing cyber security risk from hacked or compromised user and privileged accounts, according to the latest research by Cybersecurity Ventures.

The research notes that more than 3 billion user credentials/passwords were stolen in 2016. That breaks down to 8.2 million credentials and passwords stolen every day or 95 credentials and passwords stolen every second.

Based on the accelerating frequency and growing costs of security breaches, Cybersecurity Ventures predicts \$6 trillion annually in cybercrime damage by 2021!

Statistical analysis suggests almost everyone connected to the Internet has had their credentials/password stolen and a staggering 3 out of 7 people on earth have already had their credentials/passwords stolen at some point.

Charged with defending enterprise customers, employees, IoT devices—and most importantly privileged account users—from compromise and identity theft, cybersecurity professionals must raise awareness about protecting passwords, and help change user behaviors by leveraging more effective, automated IT solutions.

This report aims to assist cyber defenders and educate the wider global community through a statistical analysis of the massive password expansion and associated challenges that lie ahead. Some vendors—such as AT&T—have suggested a future with no more passwords.⁽¹⁾ But, while eliminating passwords may be possible one day, that scenario will not likely be realized for many years, if at all.

In spite of the considerable efforts to replace passwords, they are the dominant form of authentication on the web and are likely to remain so. Some researchers argue that “no other single technology matches their combination of cost, immediacy and convenience” and that “passwords are themselves the best fit for many of the scenarios in which they are currently used.”⁽²⁾

GLOBAL PASSWORD “ATTACK SURFACE” WIDENS WITH 4 BILLION PEOPLE ONLINE BY 2020

User names and passwords are designed to protect the identity of people and machines, allowing exclusive access to IT accounts that manage and control our lives. Both human and machine accounts have inevitably multiplied with the growth of Internet connections we consider so vital to conducting our personal and professional business activities.

According to the Microsoft Secure Blog, four billion people will be actively online by 2020.⁽³⁾ Chances are most, if not all, of those people will need several user names and passwords as credentials for accessing multiple online accounts. Numerous IT industry reports estimate that users can average as many as 36 passwords each. While there is no universal agreement about the number of passwords per user, this report considers 25 passwords per user as a conservative number.

Based on this assumption, Cybersecurity Ventures estimates that by 2020 there will be at least 100 billion human passwords requiring cyber protection.

SOCIAL MEDIA A BIG CONTRIBUTOR TO PASSWORD GROWTH

Social media usage is continuing to explode, says Joseph Steinberg, an *Inc. Magazine* contributor covering cybersecurity, and an expert on social media security.

Steinberg shares the following counts for the most popular social media properties:

Facebook – About 1.79 billion active monthly accounts (self-reported)

Twitter – About 313 million monthly active users (self-reported)

Instagram – About 500 million users (self-reported, number of active is relatively high)

LinkedIn – About 467 million users (self-reported, how many are active has been speculated to be significantly lower)

Social media use will continue to grow according to Steinberg. He expects all the major established platforms to continue adding users, and emerging platforms such as musical.ly to grow even more rapidly.

THE INTERNET OF THINGS (IOT) MEANS BILLIONS MORE MACHINE PASSWORDS

The number of IoT devices is estimated to grow from 15 billion in 2015 to 200 billion by 2020, based on projections by tech giant Intel Corp., market researcher IDC, and the United Nations.⁽⁴⁾

While not all IoT devices will have an actual password, they will need an authentication method and will likely store a key or password within the configuration that connects them to a network, explains leading Privileged Access Management (PAM) experts at Thycotic.

“Any IoT device that has an interface will have a password protecting the interface that allows it to be configured,” says Joseph Carson, a Thycotic cybersecurity expert with twenty-five years’ experience in enterprise security and infrastructure. “Plus, any Bluetooth capable device like wearables will use a PIN for a passcode.”

Based on a very conservative estimate of one-password-per-machine, Cybersecurity Ventures estimates 200 billion machine passwords will need to be secured by 2020.

TOTAL PASSWORDS NEEDING PROTECTION TO TOP 300 BILLION BY 2020

Cybersecurity Ventures projects the total number of user and privileged accounts that will need to be secured—which is a combination of human and machine passwords—will surpass 300 billion passwords by 2020. While there is clearly a margin of error based on several variables—most notably the number of IoT devices—the password attack surface will inevitably grow by an order of magnitude over the next 4 years.

As Passwords Multiply, So Do the Risks

Unfortunately, human passwords are often the most vulnerable credentials targeted by hackers. That's because human passwords typically are easy to "crack" with software that automates the process of guessing passwords by exploring countless combinations in very short periods of time. And in many cases, humans use the same password for many of their online accounts as an easy way to remember them. Once cracked, these passwords give hackers the "keys to the kingdom," allowing them access to steal or manipulate proprietary information.

A security awareness campaign run by the UK government in 2014 concluded that the average person in Great Britain has 19 passwords to remember. Yet, current data shows that only 35 percent of Britons are following their government's latest advice to protect their accounts from cybercrime by using strong passwords composed of three random words.⁽⁵⁾

LOTS OF OPPORTUNITY TO COMPROMISE PASSWORDS

Companies on the Fortune 500 list in 2015, for example, employed a combined total of 27 million people. Thycotic experts estimate that these employees in 2020 will have an average of 90 accounts (combination of business and personal) requiring login IDs and passwords. That would put the total number of passwords belonging to Fortune 500 employees at 5.4 billion in 2020.

While employees have their own login credentials -- there's a proportionately small number of privileged users (typically IT and system administrators) who each have access to hundreds, and sometimes thousands, of login IDs and passwords.

Approximately five percent of Fortune 500 employees are privileged users, putting the number of people with privileged account access at 1.35 million. These numbers provide a huge opportunity that hackers love to exploit.

A recent report from the National Institute of Standards and Technology (NIST) revealed that most human account users are suffering from security fatigue—defined as a weariness or reluctance to deal with computer security.⁽⁶⁾ The study notes that the average computer users felt overwhelmed and bombarded, and they feel tired of being on constant alert, adopting safe behavior, and trying to understand the nuances of online security issues. When asked to make more computer security decisions than they can manage, users experience decision fatigue, which leads to "security fatigue."

Typical examples of security fatigue include being tired of remembering usernames, passwords, PIN numbers, navigating multiple security measures, and account lockouts due to incorrectly entered passwords. The study also found that users believe safeguarding data is someone else's responsibility, and users questioned how they could effectively protect their data when large organizations frequently fall victim to cyber-attacks.

SOCIAL MEDIA EXTENDS THE RISKS

According to Thycotic experts, social media platforms introduce significant risks due to the extensive use of what are known as social logon's or application passwords. To avoid users having to remember multiple passwords for social media accounts, new platforms allow for a single logon to be linked to these accounts. However, these platforms often share customer data without clear transparency to the user.

The sharing of information on social media can often lead to identity theft, virtual kidnapping, or spear phishing against one's friends, colleagues, or relatives. On many social media platforms, it's also easy to create fake accounts and/or impersonate others. Furthermore, some people steal others' photos and present them as their own, or utilize them for nefarious purposes such as using someone else's photo in an ad for an online hookup site.

On top of this, most social media users do not use multi-factor authentication for logging into social media sites, and many people use weak or reused passwords—putting their accounts at risk of being taken over by hackers.

Thus, a breach at one site can easily lead to accounts being taken over at other sites. Because many people use Facebook or Twitter authentication and passwords for multiple sites, a takeover of one's Facebook or Twitter account can, in fact, mean the compromise of many other accounts as well. And, when a hacker takes over a Facebook or Twitter account, the hacker can readily social engineer attacks on the victim's colleagues, friends, and relatives.

2016 BREACH DISCLOSURES BIGGEST IN HISTORY

Yahoo – 1 billion credentials/passwords compromised Dec 2016; 500 million user account credentials reported stolen August 2016

Dropbox – 68 million credentials and passwords

LinkedIn – 117 million credentials and passwords

Multiple Email Providers - 270 million credentials and passwords (57m mail.ru , 40m Yahoo, 33m Hotmail, 24m Gmail)

Rambler – 100 million credentials and passwords in clear text

MySpace – 470 million passwords

Friend Finder Network – 412 million in customer data

These high-profile breaches alone add up to nearly 3 billion stolen credentials and passwords. That works out to 5,700 passwords compromised every minute or 95 passwords disclosed per second this year.

MACHINE PASSWORDS JUST AS VULNERABLE

Machines accessed by passwords are the lifeblood of our connected world, especially for businesses operating globally. Numerous schemes are constantly being devised to fool everyday users into revealing their usernames and passwords. Once compromised the user account opens the door for hackers to exploit unauthorized access to all kinds of information.

That's because for most attackers taking over low-level user accounts is only a first step. They use that initial user account to "leap frog" across the IT infrastructure and eventually take over privileged accounts so they can escalate their access to applications, data, and key administrative functions. After they gain access to privileged account credentials, hackers can easily conceal their activities in the guise of a legitimate administrative user.

Because privileged accounts are used by systems administrators to deploy and maintain IT systems, they exist in nearly every connected device, server, database, and application. In addition, privileged accounts extend well beyond an organization's traditional IT infrastructure to include employee-managed corporate social media accounts.

Thus, privileged account passwords are prime targets for hackers for good reasons. One privileged account password breach can allow a hacker to access and steal the credentials and passwords belonging to every employee in a company. Even in the most sophisticated IT environments, privileged accounts are all too often managed by using common passwords across multiple systems, unauthorized sharing of credentials, and default passwords that are never changed—making them easy targets to compromise.

YAHOO BREACH OF 1 BILLION USERS LARGEST IN HISTORY

In December 2016, it was revealed that more than one billion user accounts had been disclosed and impacted by a breach at Yahoo. Combined with other major breaches this year, the Yahoo breach brings the total number of stolen credentials and passwords to more than 3 billion—an amount nearly equal to the number of people actually using the Internet, according to Thycotic's Joseph Carson. He notes that publicly disclosed information indicates the breach probably resulted from privileged unauthorized third party access. This has been a common source of many of the data breaches this year. According to the latest Ponemon breach study the average cost per stolen record containing sensitive data is \$156. That would put the potential cost of the Yahoo breach at approximately \$156 billion USD, and the combined breaches potential cost at \$234 billion USD. ⁽⁷⁾

PASSWORD THEFT A PRIME CULPRIT FOR TRILLIONS OF DOLLARS IN CYBERCRIME DAMAGES

According to the latest Verizon Data Breach Investigations (DIBR) Report, 63% of data breaches are a result of stolen and weak credentials and passwords. That reinforces a recent story published in the Intel IT Peer Network that maintains the biggest IT security threats heading into 2017 are data breaches resulting in stolen data—breaches that usually begin with a stolen username and password.⁽⁸⁾

The 2016 Verizon DBIR estimated that a data breach of 100M records ranges from \$5M to \$15.6M per breach based on the ITRC's 2015 data breach. The report concluded that businesses suffered nearly \$3 billion in damages to their operations and brands in 2015 alone. Given the massive expansion of the cyber-attack surface in coming years, Cybersecurity Ventures predicts this number to grow to over \$6 trillion annually in cybercrime damage by 2021, based on the accelerating frequency and growing costs of security breaches.

“The 2015 Verizon Data Breach Investigations Report estimated that more than 60% of corporate breaches are tied to compromised identity with a key culprit being stolen username and passwords or misused credentials” summarized Tom Garrison, Vice President and General Manager, Business Client Platform Division, PC Client Group at Intel Corporation.⁽⁸⁾

The message could not be clearer. Effective password security—especially for Privileged Accounts—can mean the difference between a simple perimeter breach and a cyber catastrophe that results in billions of dollars in damages. Most companies and consumers today are not doing enough to protect their passwords, giving attackers easy access to sensitive data and critical systems. It is important to immediately start improving and utilizing best-in-class technologies or by 2020 their password security problem could easily quadruple in size. That's a scenario that few of us want to contemplate let alone experience. **The time to act is now.**

References

- 1- <https://www.forbes.com/sites/stevemorgan/2016/05/05/att-no-more-passwords-pin-codes-and-security-questions/#773044c97293>
- 2- https://en.wikipedia.org/wiki/Password#cite_note-68 [68]
- 3- <https://blogs.microsoft.com/microsoftsecure/2016/01/27/the-emerging-era-of-cyber-defense-and-cybercrime/>
- 4- <http://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png>
- 5- <https://www.cyberaware.gov.uk/blog/only-35-britons-followinggovernments-latest-password-advice> and <https://www.cyberaware.gov.uk/blog/three-random-words>
- 6- <https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly>
- 7- <https://www.scmagazine.com/data-on-1b-yahoo-users-stolenin-second-breach/article/579323/>
- 8- <http://itpeernetwork.intel.com/intel-business-pc-vp-tom-garrison-tackles-identity-access-security/>

Steven C. Morgan, Editor-In-Chief

Founder and CEO at Cybersecurity Ventures, and Editor-In-Chief of the Cybersecurity Market Report and the Cybersecurity 500 list of the world's hottest and most innovative cybersecurity companies. Steve writes the weekly Cybersecurity Business Report for IDG's CSO, and he is a contributing writer for several business, technology, and cybersecurity media properties.