Empowering the Weakest Link in Today's Technology with: Cyber-security Protection by Means of Password Security

Lázaro R. Serrano Malavé
Master in Computer Science
Advisor: Dr. Nelliud Torres
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— No matter how expensive or how advanced the technology inside your organization is, there is always going to be the human factor. In this project I develop a program written in C++ that will help not only IT professionals but also the general public that use passwords to log in to their work environment. This software will prompt the user to enter a password and the program will then give the user a password score while suggesting the user to add certain ASCII characters to help strengthen their password and try again, as well as displaying how many years it would take for a super computer to crack the user's password. With 81% of hacking-related breaches being generated because of stolen and/or weak passwords, it is important for users to have a well-constructed password to avoid being the target of a criminal hacker.*

Key Terms *— Cybersecurity, Cybersecurity Awareness, Cyber-threat, Password Analyzer.*

INTRODUCTION

We are currently living in an era where technology is found in every aspect of our lives. And with great advances comes great responsibility. Where ever there are people working hard to achieve their goals there will always be one other group of people with a different goal in mind, ransack organizations and individuals alike. These individuals will try to penetrate your systems with the purpose of stealing your information for their own personal use or to trade stolen information for resources. These individuals are known as malicious hackers. To defend off against these types of groups, individuals and organizations alike will need to not only be highly trained against emerging threats, yet they will need to acquire certain tools and software that will help protect their computer systems from the theft of information and data.

LITERATURE REVISION

There are various types of attacks such as Distributed Denial of Service, Waterhole attacks, Fake WAP, Ransomware, Phishing, Trojans and other types of malware just to name a few [1]. In this paper I will be discussing more in depth the topic of password security. Every person has had to create a password either if it is for their mobile device, computer at work or even their secret pin number for their debit card. At the moment of creating these passwords, users will often use their own personal name, pet name or other easy to guess words followed by a few digits. This is considered a weak and not a recommended way to construct your password. A strong password will take millions and millions of years, the world would come to an end and with today's technology the password will not be able to be cracked by the brute-force technique. To create a strong password the user must make sure to include: lower case letters, upper case letters, digits, special symbols and a length no less than 8 characters while I recommend a length of no less than 16. If the user successfully includes these 5 elements, then a malicious hacker would need to go through 95 different possible characters for each character in the password string. For example, if the password had 16 characters, the hacker would need to go through forty-four nonillion, twelve octillion, six hundred sixty-six septillion, eight hundred sixty-five sextillion, one hundred seventy-six quintillion, five hundred sixty-nine quadrillion, seven hundred seventy-five trillion, five hundred forty-three billion, two hundred twelve million, eight hundred ninety thousand, six hundred twenty-five

(4401266686517656977554321289062 5) different password combinations to be able to successfully brute-force your password, yes it is mathematically impossible [2]. The table below will give you a broader view of these numbers [3].

Table 1
Distinct Possible Combinations for a Fixed String Length with 93 Unique Printable Characters in the ASCII Set

Exponential Form	Scientific notation	Standard notation
93^8	5.60E+015	5595818096650401
93^9	5.20E+017	520411082988487293
93^{10}	4.84E+019	48398230717929318249
93^{11}	4.50E+021	4501035456767426597157
93^{12}	4.19E+023	418596297479370673535601
93^{13}	3.89E+025	3892945566558147263881089 3
93^{14}	3.62E+027	3620439376899076955409413 049
93^{15}	3.37E+029	3367008620516141568530754 13557
93^{16}	3.13E+031	3131318017080011658733601 3460801

If a user named Linda were to create a password for her corporate email, and decides to use the password linda321, then most email service providers will accept Linda's password, since it has a minimum of 8-character length which is also the National Institute of Standards and Technology's minimum requirements recently stated in the document SP 800-63B. The password Linda provided only makes use of two of the four basic characters for password creation. The two-character groups this person provided were lower case letters and digits, while failing to include upper case letters, special symbols and a larger length. If a malicious hacker were to try and brute-force Linda's password, it would not take long before the credentials are cracked. Since Linda only used lower case and digits, there is only a total of 36 different possible characters per character in the password string, 26 lower case characters and 10-digit characters [4].

During a recent study carried out by the multinational cyber-security and anti-virus provider known as Kaspersky Labs has recently stated that the US government spends over $13 billion each year on cyber-security related services and tools, yet they assure cyber threats will continue to grow at a swift pace [5]. For this reason, the National Institute of Standards and Technology (NIST) recommends organizations, small or large alike, to obtain monitoring services in real-time for all of their electronic resources, especially those assets that store and process confident information and data. Today's cyber criminals have the power to take down large company's by penetrating and stealing confidential information such as the organizations client's social security numbers, credit card information and other personal data. Thefts like these are the reason why company's no matter the size should have a cyber-security service provider to help them with any vulnerabilities their systems may have to help prevent and detect any malicious and unwanted activities inside your network. With real-time infrastructure and device monitoring, organizations will be notified by their Managed Security Service Provider (MSSP) about any passwords that have been utilized in any unsafe website such as websites with no Secure Socket Layer (SSL) certificate available. Websites that do not have an SSL certificate are less trusted and are not recommended to enter any personal credentials as non-HTTPS websites are not encrypted and unsafe as a malicious hacker could get his hands on this confident data. Another threat that a real-time MSSP will notify their clients on are large brute force attempts when entering a user's credentials. Password theft is just one of the many threats an MSSP will help an organization's cyber-security needs.

There are two types of threats, internal threats and external threats. Internal threats are those threats that come from inside the organization's network while the external threats and attacks come from outside an organization's network. The internal network will have a range of internet protocols (IP's) ranging from 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255 and from 192.168.0.0 to 192.168.255.255. The organizations that distribute IP addresses throughout the world are the ones who provide the range of IP addresses for private networks. Since more than one person can have the same private IP

inside different networks, private IP's are not traceable and non-routable, so online tools that track your geolocation as well as other important information by looking up certain IP addresses will not be able to do so. When a threat or attack is internal, then there are two possibilities, either it is a false positive or the malicious hacker has taken control from inside the network. These internal threats are harder to detect and, in most cases, will happen because an employee downloads a file with attachments that will facilitate the hacker's access into their company's network. Many firewalls and anti-virus software's block external or unknown IP addresses while giving full access to internal IP addresses. The problem with this type of access is that if there is an infected computer inside your network, the hacker may use it to carry out brute-force attacks without being detected.

Many corporations have recently been adding a second layer of authentication for their employees during their time of login. This second layer of authentication is called two-factor authentication and will provide a larger level of authentication for the user. Two-factor authentication or 2FA for short, will work as an additional later of security which works in a way that the usual login credentials will not suffice. The way that 2FA works is when the user who enters his or her credentials to login such as their username and password onto a particular page or work space, the application will prompt the user to enter the additional piece of login information which only, and only that user will have on them in their immediate reach such as a password, a smart card ID, a biometric identifier, etc... One of the more secure and widely used two-factor authentication technique involves the use of the employee's mobile phone. In this particular 2FA technique when the user enters his or her login credentials onto a system, the system will send a text message to that particular user's mobile phone with a one-time use code which is typically a four to six-digit passcode which will expire in an assigned amount of time such as 60 seconds. This 2FA technique uses your mobile phone to authenticate which is convenient since nowadays every person carries around with their mobile phone. Mobile phone two-factor authentication is also a great tool since the passcode that is send to the mobile device is always changing and expires in a certain amount of time. This form of authentication will definitely lower the amount of identity theft cases for your organization as well as other threats such as phishing since even if the malicious hacker steals your credentials, he would still need physical access to your personal mobile phone. Although this particular technique for two-factor authentication may sound flawless and convenient, there are some drawbacks such as a user is going to need to carry his mobile device at all times and make sure it has enough battery and phone signal to receive the messages and that user must make sure that he or she has a plan with unlimited receiving text messages on their phone. Another factor would be if you are to lose your mobile device or if it has been damaged, then that user would need to get access to a new phone with the same phone number to be able to receive these passcodes that the system will send to their device [6]. The purpose of having a strong base in cyber-security is to be skilled when working in the field of information technology. Information technology has a broad field and a very important topic which makes up a large part of every organization. Since attackers or hackers are always on the lookout to cause harm to other people's computers or networks it is important to stay up to date with any changes in software as well as any changes to hardware while making sure the security programs you work with are on the most recent patch. One model that is well known to help protect your company and organization is the CIA security triad which are three components and is also known as the AIC security triad. These components are the following: confidentiality, integrity and availability. This model is widely used to help guide policies on information security within an organization. This triangle is still used today since it manages to accomplish its tasks concerning the mayor problems of vulnerability in systems that work and manage information and data. The purpose for this model is to guide policies for information security inside of an organization. The CIA triangle or CIA

Triad stands for Confidentiality, Integrity and Availability. In the confidentiality branch, the model describes on how you can protect against the loss of confidentiality by ensuring that users who are not authorized to enter a particular area, do not enter. In other words, only users who do have the authority to enter, may enter while those that do not have authority do not. The integrity branch describes on how to prevent those users that are not authorized or who do not have permission to modify any data in a system do not [7]. Some techniques to prevent this is hashing, and audit logging. An audit log is also known as an audit trail and is often used in information security, as it keeps a chronological record that provides evidence of the activity that is happening at any given time or location. If there is a missing file or a deleted file yet the company does not know who or why that event was taken place, they may verify the audit trail to see the exact user as well as the time frame each user was logged in at the time. The final branch is availability, this branch discusses on how to prevent the loss of availability which guarantees that systems and data in those systems are available when they are going to be needed.

It is important to have different levels of permissions and access control; some low-level employees may want to access areas inside a network where they have no business visiting. This action is considered unnecessary and may cause harm to the organization if the employee modifies any existing file as well as creating or destroying any information or data in which that user is not supposed to, whether it is on purpose or by mistake. Either way it is crucial to the organization, so a good way to prevent these types of actions from happening is by giving permission and authorization to only those who really need to access certain areas inside the network such as a server or database. In information security, access control is selective restriction of access to a certain place or resources [8]. Information and data are very important inside of every company and organization. Then depending on what position a specific employee holds inside the company, he or she will be able to work with this information, whether it is classified information or unclassified information, this will drastically reduce the window of human error. As described previously, authentication is often described as when users have to provide an amount of information to be able to access a certain area. For example, a username and password are a common technique in most if not all organizations worldwide. It has been proven that multiple factor authentication is a strong mechanism, nonetheless employees must be aware and trained on taking safe security measures. Passwords are one of the weakest forms of authentication. Static passwords may not be secure since they stay the same over a large period of time while the dynamic passwords keep on refreshing and changing their password every time the user times out the session [9]. Even though the dynamic type may sound better it carries with it a larger amount of risk since you will need to remember the code more often than in the static type password method. On the other hand, cognitive passwords which test personal things for example: the name of your dog, your mother's maiden name or what city you were born, are a kind of password that you will never forget yet very few people will know since it uses up information from your personal matters. Another form of accessing certain areas within your network is with single sign-on which stands for SSO. Single sign-on refers to a session and a user authentication service that grants a user access to different kinds of applications while only having to authenticate once instead of having to enter the user's credentials for each of the applications [10]. There are various positive factors for integrating SSO properties into your organization, one factor is not having to remember so many different passwords and which should be use where. With SSO you will only need to enter your credentials once and will be able to browse all other applications with easy. Another factor where SSO will help benefit your company is productivity, now that you only need to login once and then have access to as many applications as you need to use during your work day, then you will save a large amount of time every single day you login using the SSO implementation.

Using certain security tools will not only help preserve a wide variety of useful qualities such as the integrity of your company but also protect it from being the victim of potential corporate collapse. A corporate collapse could happen to any organization no matter how big or small it could be. A corporate collapse will usually occur when a company or organization falls into bankruptcy. An organization can fall into bankruptcy by poor management inside the company but it could also fall into bankruptcy by means of it being the target of a malicious cyber-attack. Every day technology is becoming more and more sophisticated whole the malicious hacker's attacks continue to grow as well [11]. Many small companies that fall target to a cyber-attack usually go out of business within months. Most companies do not have any type of cyber-security awareness training when their employees join their organization nor during a regular basis of working inside the company [12]. Without proper training and organization inside a company, even the lowest level employee can bring down a company without doing it on purpose. For example, if one of the employees receives an email that appears to be from a legit source and proceeds to click on the link, then it could very well be a malicious link that even though it does not appear to be threatening, that user has just downloaded malware which could spread through the whole company's network while infecting other computers and just like that, credit card information, social security numbers, and much more confidential information and data stolen by a single click. It was recently posted by the U.S. National Cyber Security Alliance that 60 percent of small businesses cannot sustain their businesses over a period of six months after a cyber-attack. Many cyber criminals decide to target small businesses as most are not yet aware of these types of vulnerabilities or simply because of the lack of resources in the company to provide their employees with cyber-security awareness training. These types of risks are the reason why companies and organizations need to invest in educating their employees and obtaining tools to help fend off against these types of attacks and vulnerabilities.

METHODOLOGY

In this paper I discuss how a password analyzer can help all organizations, from small companies to large corporations. The way this password analyzer works is by first asking a user to enter a password that has at least an eight-character length, if the length falls short then it will prompt the user to re-enter his or her password once again. Once the user enters a valid password string the program will then provide: suggestions on how to edit your current password to make it an even stronger one.

```
if(upper == false || upperCount < 4)
    cout << "- Add upper case letter(s) to your password" << endl;
if(lower == false || lowerCount < 4)
    cout << "- Add lower case letter(s) to your password" << endl;
if(digit == false || digitCount < 4)
    cout << "- Add digit(s) to your password" << endl;
if(symbol == false || symbolCount < 4)
    cout << "- Add symbol(s) to your password" << endl;
```

Figure 1

Displays Code Written in C++ on How the Program Alerts the User to Modify Entered Password String

The program will then provide a password score breakdown that will give the user a password score to see how well he or she did and how long it will take in years, for the world's fastest computer to brute-force the users password. After the software is done analyzing, it will then ask the user if he or she would like to run the program once again so that the user can create a stronger password using the advice and suggestions provided. The user will be able to continue this process as long as he or she would like, or until the user receives a total score of 100%.

There is a total of 128 unique ASCII characters, yet out of the 128 characters only 95 are printable characters. The set of printable characters are used to represent a written symbol or text inside a document or a programs code. The amount of printable characters that I have implemented and included in my software has a total of 93 unique printable ASCII characters. These 93 unique characters are composed by the following: lower case letter characters which contain a total of 26 unique characters, upper case letter characters which contain a total of 26 unique characters, digit

characters which contain a total of 10 unique characters and special symbols which contain a total of 31 unique characters. To calculate the amount of years it would take for the user's entered password string to be cracked we would use the following formula: (((93^(Password Length)) / 350,000,000,000) / (60*60*24*365)). For a better view at this formula please see image below.

$$\frac{93^{\text{Password Length}}}{(350{,}000{,}000{,}000) \times 60 \times 60 \times 24 \times 365}$$

Figure 2
Formula to Calculate in Years, How Much Time it Would Take to Successfully Brute-Force a User's Password

Let me describe this formula by parts, the first part containing (93^(Password Length)) will be the amount of unique characters which is 93 elevated to the power of the password length. The number three hundred fifty billion (350,000,000,000) is the amount of guesses the world's fastest computer can cycle each second [13]. That is a total of 21,000,000,000,000 guesses per minute! The last segment of the formula (60*60*24*365) will consist in the conversion from years to seconds where there are 60 seconds in a minute, 60 minutes in an hour, 24 hours in a day and 365 days in one year, which is a total of 31,536,000 seconds each year. When multiplying 350 billion times the number of seconds in a year, we will have the total amount of password guesses per year. The amount of different password combinations divided by the total amount of guesses per year will be how many years it would take to successfully brute-force the user's password string.

RESULTS

After the Password Analyzer was complete and ready to begin testing user's password strings, I put the software to action by selecting five users at random, from low level cyber-security skills up until highly trained specialists. I began to notice that just after the first try, the users began to take the suggestions provided by the analyzer and after running the software for the second time, 80% of the participant's password string became stronger. We can notice in the images below how one participant increased his score during his first run compared to his final run.

```
Your password: 'Camper324' fits the standards
yet below is a list of items that could improved
your password strength:
- Add upper case letter(s) to your password
- Add digit(s) to your password
- Add symbol(s) to your password
- Add additional characters to lengthen your password

Score Breakdown:

Upper-case points: 10/20
Lower-case points: 20/20
Digits points: 18/20
Symbol points: 0/20
Length points: 4/20

You obtained a total score of: 52% F
```

Figure 3
Participant's First Execution

```
Your password: 'Coconut787#$%' fits the standards
yet below is a list of items that could improved
your password strength:
- Add upper case letter(s) to your password
- Add digit(s) to your password
- Add symbol(s) to your password
- Add additional characters to lengthen your password

Score Breakdown:

Upper-case points: 10/20
Lower-case points: 20/20
Digits points: 18/20
Symbol points: 18/20
Length points: 15/20

You obtained a total score of: 81% B
```

Figure 4
Participant's Final Execution

There was only one participant that began strong with a score of 79 yet maintained a constant score of 79 through their first through third attempt. There was also an increase in 100% of the participants when comparing their first attempt to their fifth and final attempt.

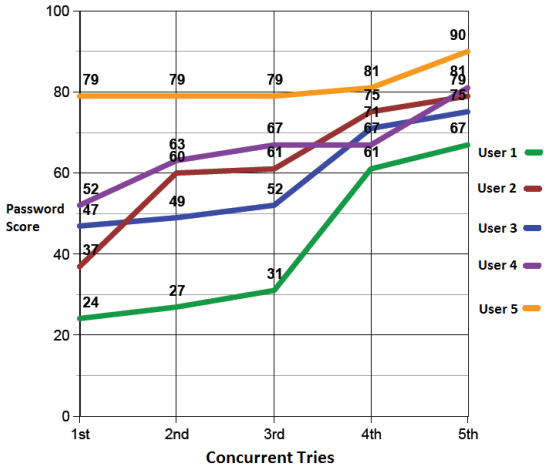

Figure 5
Results after Entering the User's Password Five Times while Applying the Recommendations

We can notice in the graph above that all of the different user's password strings increased in strength after reading and applying the Password Analyzer's recommendations [14].

Guidelines

When running this software for the first time it is important to know what your main goal is. The main goal for the individual executing the code is to create a strong password string while modifying that existing password by adding the suggestions found in the figure below for example.

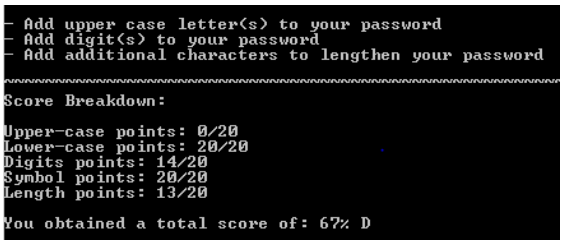

Figure 6
Suggestions made to the User after Running the Password Analyzer

When typing in the string, the analyzer will prompt the user to enter a string with a minimum of eight characters, after the eight characters or more string has been input, the user will then hit enter to pass onto the next screen, which will display suggestions on how that user can modify their existing password to create an even stronger password. The next screen will then display a password score from a minimum of 0% being the worst score up until a 100% which will be the highest score possible. In addition to the password score, the Password Analyzer will output to the user how many years it would take for that password to be cracked using the world's most sophisticated super computers.

CONCLUSION

There has been an increase in cyber-security awareness throughout the years inside companies and organizations as well as general individuals [15]. With so many people taking action and applying defenses against cyber-attacks the number of victims all from large corporations to small industries will in fact be more prepared and less likely to become a vulnerable pray. Even with more and more entities absorbing knowledge and inquiring cyber-security tools, malicious hackers will not stop, yet they will continue to construct new and even more sophisticated methods of penetrating your systems. This is why it is important to stay informed about any new and emerging threats and vulnerabilities.

ACKNOWLEDGEMENTS

I would like to thank our current director of our master's program, Dr. Alfredo Cruz.

I would also like to thank my mentor Dr. Nelliud Torres for guiding me throughout this whole project.

And a special thank you to all the graduate school staff for guiding me through this process.

REFERENCES

[1] Secureworks. (2017, May 12). *Cyber threat Basics, Types of Threats, Intelligence & Best Practices* [Online]. Available: https://www.secureworks.com/blog/cyber-threat-basics.

[2] E. Furey. (2017, July 2). *Numbers to Words Converter* [Online]. Available: https://www.calculatorsoup.com/calculators/conversions/numberstowords.php.

[3] E. Rabbit. (2005, Nov. 13). *100 Digit Calculator* [Online]. Available: http://rabbit.eng.miami.edu/class/een218/calculator.html.

[4] P. Grassi. (2017, Dec. 1). *"Digital Identity Guidelines" NIST Special Publication 800-63B* [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

[5] Kaspersky. (2017, Apr. 28). *What Is Cyber-Security?* [Online]. Available: www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

[6] Securenvoy. (2012, May 31). What Is Two Factor Authentication? [Online]. Available: www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm.

[7] M. Rouse. (2014, Nov. 21). *What Is Confidentiality, Integrity, and Availability (CIA Triad)?* [Online]. Available: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.

[8] M. Rouse. (2014, June 30). *What is Access Control?* [Online]. Available: https://searchsecurity.techtarget.com/definition/access-control.

[9] P. Portalguard. (2016, Mar. 11). *The Future of Authentication* [Online]. Available: https://www.portalguard.com/blog/2016/03/11/static-password-part-ii-dynamic-password.

[10] N. Torres. (2006, Dec. 11). *El Uso De Portales Corporativos En La Gerencia Del Conocimiento Para Las Empresas* [Online]. Available: http://docplayer.es/839223-El-uso-de-portales-corporativos-en-la-gerencia-del-conocimiento-para-las-empresas.html#show_full_text.

[11] G. Miller. (2017, Mar. 24). *60% Of Small Companies That Suffer a Cyber Attack Are out of Business within Six Months* [Online]. Available: www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business.

[12] M. Zacharia. (2010, Sep. 16). *Cyber security Training for Employees: Guidelines* [Online]. Available: https://www.computerweekly.com/tip/Cyber-security-training-for-employees-Guidelines.

[13] J. Samborski. (2015, Dec. 16). *Hi-Tech Guessing Game: 350 Billion Passwords A Second* [Online]. Available: https://www.scientificcomputing.com/blog/2015/12/hi-tech-guessing-game-350-billion-passwords-second.

[14] IES. (2010, Mar. 9). *Create A Graph* [Online]. Available: https://nces.ed.gov/nceskids/createagraph.

[15] D. Bonderud. (2017, Oct. 2). *National Cyber Security Awareness Month: The 2017 Outlook* [Online]. Available: https://securityintelligence.com/national-cyber-security-awareness-month-the-2017-outlook.