CRYPTOGRAPHICALLY USE OF CAESAR CIPHER TECHNIQUE IN PASSWORD MANAGING AND SECURITY SYSTEM

PRASHANT KUMAR DEY

Department of Electronics, KIIT University,
Bhubaneshwar – 751024, India
E-mail: prashantsavior@gmail.com

TARUN KUMAR DEY

University Department of Physics, B. R. A. Bihar University,
Muzaffarpur – 842001, India
E-mail: tkdeyphy@gmail.com

Abstract

In this paper we introduced a new type of social engineering attack via the website. We computed the result and then proposed a method to mitigate that attack. The research objective followed by the description of the experiment and then the mitigation of the suggested attack. The results were properly tabulated and contained the observations of our results. The paper ends with using the Caesar cipher for introducing the new password set method and its uniqueness.

Keywords*:* Security, Social engineering attack, Vulnerability, Mitigation, Encryption.

1. Introduction

Social Engineering Attack (SEA) is the art of exploiting the weakest link of information security systems i.e., the people who are using them. It is a method of gathering information and then performing attacks against the gathered information and Information Systems. This attacks results in a huge amount of loss on any individual's life. SEA mainly occurs due to the low awareness of people regarding the digital life. This can be identified using the neural network [1]. The objective of this research is to introduce a new type of social engineering attack, computing the result and then produce a method to mitigate the attack. A thorough study was performed to take a deeper look on the aspects of SEA and then analyze it with the oldest and easiest cryptographic technique i.e., Caesar Cipher [2]. An experiment was performed in which the target people were unable about the attack and analyzing the information obtained. It is to be noted that this attack was performed only for the research and educational purpose and no information was shared or exploited with this attack. The paper begins with the research objective followed by the description of the experiment and then the mitigation of the suggested attack. The results were properly tabulated and contained the observations of our results. The paper ends with using the Caesar cipher for introducing the new password set method and its uniqueness.

2. Objective

Our aim is to demonstrate a newer form of social engineering attack and formulate a process for its mitigation. Before we introduce the newer form of SEA, lets first look into the available forms of social engineering attack like shoulder surfing, baiting, pretexting, stealing passwords, Quid Pro Quo, Tailgating, etc, out of which some of them are discussed below.

2.1. Baiting

Baiting involves the transfer of malicious software or program in order to take control over the other computer mostly for the criminal desire. It can be in the form of music, movie or games downloaded using a peer-to-peer site, or even through a USB flash drive with a company logo labeled like "Final Report on project X-2015" left out in the open for you to find. Then, once the device is used or downloaded, the person or company's computer is infected with malicious software allowing the criminal to advance into your system.

2.2. Phishing

Phishing involves false emails, chats, or websites designed to impersonate real systems with the goal of capturing sensitive data [3]. It usually mocked-up login page with all the right logos to look legitimate. It could also be a message claiming you are the "winner" of some prize or lottery coupled with a request to hand over

your bank information, or even a charity plea after a big natural disaster with instructions to wire information to the “charity/criminal”.

2.3. Pretexting

Pretexting can be referred as the human equivalent of phishing, in which a person impersonates an authority figure or someone of trust to gain access to the required login information. One can impersonate co-workers, the police, tax authorities or other seemingly legitimate people in order to gain access to your computer and information.

2.4. Quid Pro Quo

Quid Pro Quo is a request of any information in exchange for some compensation. It could be anything from goodies to real money, or a researcher asking for your password as part of an experiment in exchange for Rs 5000. If it sounds too good to be true, it is probably a quid pro quo.

2.5. Tailgating

Tailgating is when someone follows victim into a restricted area or system. This is when someone asks to hold the door open as they forgot their company RFID (Radio frequency identification) card. This could also take form as someone asking to borrow phone or laptop to perform a simple action when they are actually installing some malicious software.

2.6. Stealing Password

People have tendency to save their passwords in their browser which makes it easy to handle their various accounts [4]. At times it seems very easy to store and use it as it doesn’t require remembering the password for the different sites. But even this can be very dangerous as there are many web browser password stealers which can steal all the saved passwords.

2.7. Shoulder Surfing

In this the attacker surfs over the user in order to collect his personal information to verify whether it is used as a password or for other authentication purpose.

2.8. Dictionary Attack

A dictionary attack is an attack attempted on authentication data by trying all the possible words in a dictionary. This is not exactly a type of Social Engineering attack but it was important to mention this attack here as it is one of most efficient and frequently used attacks in present scenario. The Dictionary is mainly formed based on the information gathered through social engineering. It attempts only to a targeted list of weak passwords or on a limited number of key combinations that has a high rate of success [5]. Hence the dictionary attack is always faster than brute-force attack. It becomes easy if the password chosen is short, weak or common but it becomes very complicated and may not give result when any special characters and numbers are included as passwords. It is usually the first choice of the attacker before trying the brute-force attack. Some of the softwares used for various forms of dictionary attack are Metasploit, Brutus, Hydra, Cain & Abel, many scripting programs.

These attacks can be minimized by acting smartly and maintaining proper privacy of the information. Now days increasing number of sites and making people register in those sites can led to a new type of attack. People tend to register in many sites with the same passwords because they can’t memorize a ton of passwords for every other site. This human vulnerability can be used to exploit any person. Once an attacker came to know about this common password then he can exploit that person on various platforms. Keeping this on account, we performed an experiment in our university, targeting approximately 150 students.

3. Experimental Study

We performed a social engineering attack with the objective to know this common password. After knowing this password we tried to exploit the user to know that whether we can use those credentials to login into their email, Facebook, Twitter, LinkedIn. We found interesting results.

Our experiment started after making a website for one of the event organized in our university. In the website we asked students to register and make them their own portal after which they can use that to choose their respective country. We posted a warning message to keep the password safe from others. In the database we didn’t kept the password in the MD5 (Message Digest) hash which is the most common type of hashing technique chosen, rather we kept the password in VARCHAR so that we can have easy access to the username and password of our target. We made the registration page with the query like first name, middle name, last name, email id, username, passwords, date of birth, mobile number, alternate email address, and the security questions. Even in the security questions we entered the several security questions which were exactly in the match from the common question being asked while registering in sites like Google, Facebook etc as shown in figure 1.

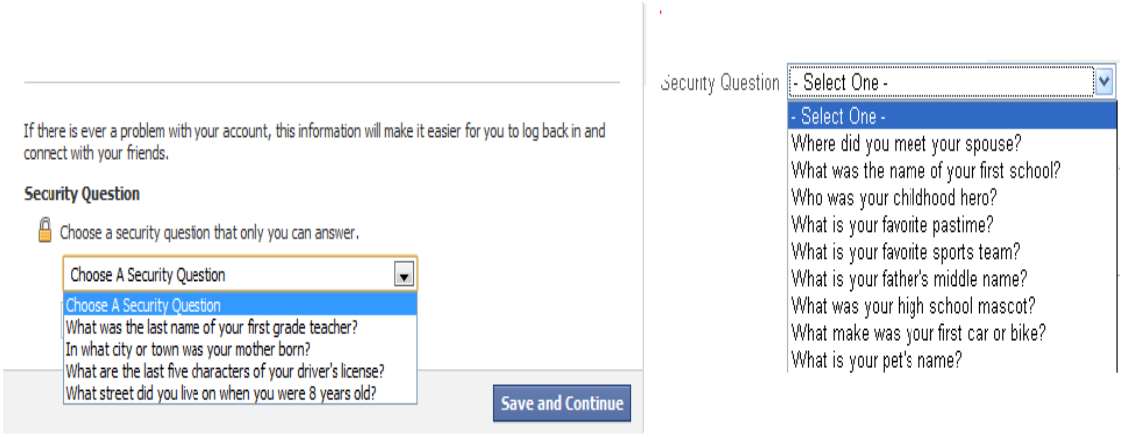

Fig. 1: General Security questions from few sites

After the people registered in the site we went through the database and downloaded it. We tried to login with that username and password in few of the frequently used sites like Gmail or Yahoo, Facebook, Twitter, Flipkart. We happen to login with few of the information and couldn't login in some of the cases. We made a graph with those reports and data. Furthermore we also used some ciphering technique to mitigate this. This attack can be made more dangerous by adding a payment gateway in the site and posing as if the person is paying with their credit/debit card for the object but actually the details are being stored in the database with the credit card/ debit card details and CVV number.
The experiment targeted 147 students and the details was tabulated in table 1.

Table 1: Students using different email provider

Total no. of subjects	**Gmail**	**Yahoo**	**Others**
147	119	9	19

Out of these 147 subjects of our study, we logged into each one's account in Facebook, Twitter, Flipkart and their corresponding email. The list is evaluated in the table 2.

Table 2: Successful login rate in different sites.

Successful Email Login	107
Successful Facebook Login	94
Successful Twitter Login	97
Successful Flipkart Login	13

The reason for low successful Flipkart login was that most of the students didn't have their account in Flipkart.

4. Method for mitigation

We will be using the Caesar cipher technique to implement a new set of passwords and make it unique for each websites and easy to remember. Caesar is one of the oldest form of encryption came into light during the World War II. It is also known as Shift Cipher [2]. In this the letter or number is rotated by some number of positions. The general Caesar cipher form is shown in table 3.

Table 3: Cryptography of a plain text using Caesar Cipher.

	ROT 1	**ROT 2**	**ROT 4**	**ROT 6**
Plain Text	PRASHANT	PRASHANT	PRASHANT	PRASHANT
Caesar Cipher	QSBTIBOU	RTCUJCPV	TVEWLERX	VXGYNGTZ

$$E(x) = x + n \quad (1)$$

$$E(x) = x - n \quad (2)$$

Equation (1) and (2) both describes about the way Caesar cipher can be set. Here 'n' denotes the number of shift and 'x' is the present letter order.

Now we will use this encryption method to modify our password combination and make it more powerful [6]. Assuming our unique password to be very strong and for this instance we took the password as "Prashant$4007". This password has the combination of alpha numeric and special symbols, even there is case change which makes it very tough for the Brute-force attacker to crack it. But since the attacker is using the website as a method to know the password so it's easy for them to know this password and can use it to exploit us. So what we are doing here is that we are encrypting this password with the uniform resource locator (URL) of the site using the Caesar cipher technique [6].

Suppose we are visiting the website facebook.com so we can encrypt our password with the URL of the site. Here we will also follow the ROT 1 method of the Caesar Cipher technique to encrypt our password [1]. The reason for following the ROT 1 method is that it is easy and fast to apply.

We will first take the two letters from our main password combination then will add an extra bit from the first character of the URL after shifting the first bit by 1. If we happen to encounter with a symbol then we will keep that as it is. Let's take that we are visiting certain website and our main password combination is Prashant$4007 [7]. The results are displayed in the table 4.

Table 4: The password combination for different sites.

Main Password Combination	Sites we are visiting	Final password combination
Prashant$4007	Facebook	Prgasfhapntb$4c00l7
Prashant$4007	Gmail	Prhasjhanntm$4b00h7
Prashant$4007	Twitter	Pruasuhasntj$4f00x7

Similarly this table can be modified by using the ROT 2 or higher rotation scheme. A person can even change the position like here we inserted after every 2 letter, one can enter after each letter or may be after 3.

5. Results and Discussion

From the above discussion we have developed a unique table for ciphering password and making it unique for each website. Even for this we don't need to remember each passwords as the password combination can be set just with the URL of the site we register into. This method not only targets on the uniqueness of the password and its memorability but also onto the increase in the strength of the passwords. We checked our password strength [8] and results were obtained from which we conclude that our password strength also got increased approximately by 10^{12} times.

Table 5: Time taken to crack the different password combinations using Brute-force [8].

Password	**Time to crack (a desktop PC) (Year)**
Prashant$4007	26×10^{6}
Prgasfhapntb$4c00l7	5×10^{18}
Prhasjhanntm$4b00h7	5×10^{18}
Pruasuhasntj$4f00x7	5×10^{18}

Although this takes a bit a time to make it come into practice but is a very safer way to have the account. Even though attacker compromises with the one account he may not have access to all other account.

6. Future Work

We are working on the program which will generate the password combinations once the people register in the site and input the URL and their password combination which will be encrypted. This program will be written in python language and will give the user right to change the value and create their own encryption method using all form of Caesar cipher method.

7. Acknowledgment

We are thankful to Dr. A K Ray, Dean of Electronics Department, Dr. Sucheta Priyabadini, Director Student Services, KIIT University and Avik Gorai, Faculty and Projector Coordinator of Department of electronics, KIIT University for proper guidance on this paper. We are also thankful to Sushant Sagar, Department of Computer Science and Souvik Hazra, Department of Electrical, KIIT University for their continuous support. We are also thankful to InternetGenx.in who provided us with hosting and domain and encouraged us in this project.

8. References

[1] Sandouka, H. Cullen, A.J., & Mann, I. “Social Engineering Detection Using Neural Networks.” In IEEE International Conference on CyberWorlds (CW’09). 2009, 273-278. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5279574
[2] Singh, Simon (2000). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. ISBN 0-385-49532-3.
[3] Halevi, T, Lewis, J., and Memon, N. Phishing, Personality Traits and Facebook. Cornell University Library. 2013. http://arxiv.org/abs/1301.7643
[4] CERT Insider Threat Team. Unintentional Insider Threats: Social Engineering. Software Engineering Institute, January 2014.
[5] Junghyun Nam, Kim-Kwang Raymond Choo, Juryon Paik, Dongho Won, "An Offline Dictionary Attack against a Three-Party Key Exchange Protocol", IEEE Communication Lett., Vol. 13, pp. 205-207, Mar. 2009.
[6] Proposed Federal Information Processing Data Encryption Standard. Federal Register (40FR12134), March 17, 1975
[7] M Zviran, WJ Haga, “A comparison of password techniques for multilevel authentication mechanisms", in Computer Journal v 36 no 3, pp 227-237, 1993
[8] Online password strength checker, https://howsecureismypassword.net