Navigating the Cyber World: Protecting Public and Private Data from Attacks

Carlos E. Morales[1] and Ricardo J. Gómez[2]

[1]Department of Information Technology, Pontifical Catholic University of Peru, Lima, Peru
[2]Department of Computer Science, National University of Engineering, Lima, Peru

ABSTRACT

In the world of Internet nothing can be done without identifying the user. Internet is borderless and to perform any task we need to give our information so that we can be identified by the Cyber world. Identity is required by any website like banking, online shopping, mails and Social sites. In general the information that is entered while registering to any website is used to identify the user for further logins and access. Some sites may ask us to create a profile which could be used by others for identification. These profiles are public and anybody can view it. This public information which we think is no where leaving us unsecured and is the key hole for the hackers to steal your private data. Now the question that the user needs to understand is *"Is my public information really Public or Private?"*

In this paper we shall study the ways the user creates his profile, the general attributes that are given while registering and few examples how the users private data can be stolen by public data. We hope the study done in this paper would create awareness to the internet users for further registrations over online.

KEY WORDS: - Attacks, Social engineering, registration methods, password policy, public data and private information

I. INTRODUCTION

According to the Internet World Stats, as of June 30, 2012, over 2.4 billion users are using the Internet and now as of June 30, 2017 the number is 3.8 billion [1] and hence the numbers no doubt will keep on increasing day to day. Now it's almost made compulsory for any user to have social accounts, online banking accounts, have an email and other personal accounts. Almost all the websites and online accounts ask user for registering before using the privileges. It won't be surprising to know that there is no online account without user registration and we can't expect even in future such a scenario of account creation without registration.

The information provided while registering for an online account usually asks for general details which we further refer to as a "Public Data". By providing this sort of information, it won't harm the user in any form. It is that feeling of a user that makes him to be careless while registration. The carelessness in creating a user profile leaks the hacker some personal information which we further refer to as "Private Data". This private data might make the hacker make use of your personal information in obtaining some documents that might ruin user's life. The three vital security issues take place every day in our world of transparent fashion, more precisely: identification, authentication and authorisation. Identification is a process that enables recognition of an entity, which may be a human, a machine, or another asset such as a software programme [2]. This identification theft has now a day became the key hole for the hackers. Our study in this regard has found some hard and most dangerous facts that inspired us in making this paper. We shall see two examples in this regard for better understanding.

In this paper we shall see how the user leaves a way to the hacker at the time of registration. We shall also see some of the techniques how the private data can be stolen from the public data. Finally we shall see some of the precautionary measures to be followed for not to make our public data reveal our private data.

II. REGISTRATION METHODS AND THE LEAK

Internet is known as a very powerful platform that changes the way we communicate and perform business transactions in current technology [3]. It has become part of everyone's life where we can't imagine a day without internet. It touched every aspect of our life wherein we perform our daily activities like online shopping, communication, bank transactions and entertainment sitting in front of a laptop. Transmitted information level is becoming more important especially as interactions that used to only be carried out offline, such as bank and commercial exchanges are now being carried out online in the form of Internet banking and electronic commercial exchanges, and damages due to such attacks will be greater [4]. In such a case where Internet has become the only means of our daily life activity, much care should be given on the security aspects on how the Internet is keeping our data secret.

When coming to security concerns many of us try to see the type of encryption and decryption followed by the site, the OTP's, email sent as a token for login and the text messages received on the mobile. When such things are received we think that the site we access is following all the safety measures in protecting our data. Many security analysis companies are only concerned on checking malicious software's, social engineering attacks, phishing, or any targeted attacks being done with the site we access. "*Insafe"* reports that more than a quarter of children in Europe have online networking profiles which can be exposed, and with over 900 million people on Facebook alone the danger is widespread [5]. Now the question arises: Is our data secured even after all these measures.

In this paper we try to understand the security of the user in another perspective. What we believe is- even though we follow all the cryptographic techniques, our data is leaving our private information to the hacker with the help of our public data. All this happens just with the data which we provide at the time of our account registration. Account creation is almost same with any site that we come across over the Internet. Users pay very less interest and attention while registering for the site. The user is asked to choose a password. If the password is not strong enough the individual is asked to choose another one. This is generally inconvenient for the user to define such a password and to remember it [6].In general they will be much eager in accessing the site and enjoying the privileges rather than paying attention towards what they are typing. Problems with password authentication, such as the number of passwords a user has to remember, strict password policies, varying systems, and memory demands will make the user pay less attention towards his password [7].

Many of the registration processes followed by almost all the sites can be precisely listed as follows

- Preferable Username and Password
- Active Email ID
- Active Mobile Number
- Date of Birth
- Job Profile
- Address for communication
- Profile Image
- Marital status
- Gender
- Face book / Twitter or other social networking sites
- Aadhar Card (In India)
- Social Security Number (Other countries)
- And Place of work / Place of study

At the first glance it just looks like a normal registration for the site. When we go into detail or when we try to combine each of them into group then the private information can be obtained i.e. when public information is combined with other public information, private data can be obtained. In the following sections we shall see few scenarios where this can be easily understood.

In most of the cases the user pays less attention while registration. Most of them will be in a hurry to use the options as early as possible from the site. We are lest bothered about the details which we are asked by the site or the application. In such a hurry user doesn't think whether the site requires those details or is it trying to get extra information from us that is really not required for the operations of the website or the application. This is the point we focus in this paper.

III. EXAMPLES OF ATTACKS CAUSED BY PUBLIC DATA

Following are two examples which help us in understanding how public data reveals our private information. We took one simple example and one complex example just to understand how the attacks can happen. Various examples can be given but we have taken only two as these may help hackers who may misuse it.

Scenario 1:- (Simple Example)

Mobile Number now a day is common for our daily use and we don't hesitate to share it to our dear ones. Sometimes other people's mobile number can be obtained from any of his registered websites like Facebook etc. Once the mobile number is known, we can see his / her profile picture and status updates from other networking sites like True Caller and Whatsapp.

Imagine an unknown person monitoring your profile picture and your status updates, pictures and messages which are personal to you and to your friends being watched without your permission. This looks simple but see how when two public information's were added (Mobile Number combined with Whatsapp / TrueCaller) give your private data.

Scenario-2:- (Complex Example)

In this example we try to see how bank account details can be hacked through your public data.

- Hacker accesses your name and date of birth from Facebook / Twitter.
- With these details he goes to the income tax site and updates them. From there he obtains the PAN Card and mobile numbers.
- Then he gets a duplicate PAN Card.
- After this he lodges a mobile theft complaint in a police station.
- With the duplicate PAN Card he gets another SIM card from the mobile service centre.
- Through the internet banking he is now ready to access your account.
- He goes to the site and uses the “forgot my password” option.
- Now he easily gets past other options and gets the internet banking pin on his SIM Card.

The hacker is now ready to access your internet banking account fully with the public data which we have provided for various sites.

Hence, all the users are requested to take enough care while registering for Facebook, Twitter with details like profile data, date of birth and mobile number.

Above examples are just for the information sake of the users and not with an intention of providing hints to the hackers. Other precautionary measure that has to be followed is listed below for the benefit of the internet users.

Figure 1:

Mail Today, New Delhi, Thursday, February 15, 2018

EXCLUSIVE

By Chayyanika Nigam in New Delhi

Hackers selling voter ID data for mere 50p

Experts say interconnection of identity papers with financial accounts has raised the risks

THANKS to the poor security system of maintaining confidential database of the citizens, after Aadhaar data leak it now appears your voter ID details can be illegally accessed and sold for 50 paise to ₹2.50.

The rates of confidential details are as low as 50 paise per information and goes up to ₹2.50. —A SOURCE

1993 was when the voter ID card was introduced in India.

Experts say easy data availability aids cyber crime

Paper clipping from English daily “Mail Today”, Article showing how private information from the public data is being siphoned.

IV. COUNTER MEASURES AND PRECAUTIONS AT THE TIME OF USER REGISTRATION

Listed below are some of the precautionary measures that can be followed for not to reveal our public data over the internet.

- The first and foremost precautionary measure that is required is the awareness of the user in creating an account online and Internet usage.
- Never give your personal credentials to anyone even to your close relations.
- Use some software’s like Trend Micro Security that helps minimize the amount of personal data tracked by websites and services. It also safeguards your accounts and ensures your data doesn’t go out without your consent.
- Learn about sites privacy and security policies. This helps us in understanding what information is collected from us, for what is it used and how safe is our data with the site.
- Bookmark frequently used sites. This helps us not to open wrong sites or Phishing sites.
- Limit our details over social websites. Since hackers first approach will be over social sites, limit the personal information as much as possible. Provide only those details which are necessary for registration.
- Avoid leaving any information about our habits and interests on any website or any social networking sites. These give a loop hole for the hacker to attract us with offers related to our interests. As we are already interested the offers might attract and tempt us to open the mails or click on a link provided.

- If a message to a cell phone is received saying that you have won a lottery and to claim it we have to provide our details like name, place, bank details and other information. In such a case before giving the details roughly by a message, ask their details first in reverse and then proceed further. In any case if it is a trap then the caller won't give any information to you.
- Make sure you use unique and long passwords
- Replacing passwords with pass codes may be a solution for these attacks. Even though the identity if stolen authentication could be impossible [8].
- Avoid using same password for multiple accounts. Use Password policy manager to efficiently handle the passwords.
- Avoid opening email attachments and clicking on malicious links.
- The other study in this regard says like this- we have used our body parts as passwords such as our voice (voice recognition), eyes (Iris), face (face recognition), and hands (Bio metric authentication). All these parts are used as passwords for our identification. All we tried is to prove ourselves to enter into our account. But what we missed here is "it is only you who can prove who you are". None in this world can be you except you. None other can think and react exactly like you. It is you who can be you in this world. "Why can't be you as your password for your Account-Self Authentication" [9].

V. CONCLUSION

As discussed, the general care and awareness of the user is the key role that plays vital in Internet usage. Knowingly or unknowingly the information provided may be giving lot of information about you which could damage us in many factors.

Even though we instruct many measures the user will be much curious about completing the registration process quickly and using the application for entertainment. Thus self control of the user is also required while playing with the Cyber world. Not only the attacker attacks with some tricks and malware's but also the attack may be with our cooperation. We may be the shareholder in the act [10] .Once the registration process is done user never tries to update it in future. Very rare the users update their profiles after registration. As it is mostly a onetime process we suggest all the users to pay enough attention while registering for any website or account. Only the necessary fields need to be mentioned at the time of registration.

Hence we hope the scenarios listed above will give a basic idea to the users how the public data is used to get your private data to the hackers. We tried to give basic idea just to create awareness to the users. Many examples can be quoted but as it will be like hints to the hackers we limited with simple examples. Hope this could help the Internet users in making them alert for the next registrations.

VI. REFERENCES

[1] Internet World Stats- Website that monitors the number of user over the Web-2017
[2] Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Jean-Jacques Schwartzmann. "A Review on Authentication Methods" Australian Journal of Basic and Applied Sciences, 2013, 7 (5), pp.95-107
[3] Z. Syed Idrus. "Database encryption for a web-based claims system". Master's thesis, School of Computer and Communication Engineering, University Malaysia Perlis, Perlis, Malaysia, 2008.
[4] R. Cha and C.W. Kim. "Password generation of OTP system using fingerprint features"- 2008 International Conference on Information Security and Assurance, page 243-247. Springer, 2008.
[5] Parris-Long. Safer internet day: "Why every generation has a role to play in keeping the web secure", Retrieved on 10 February 2012. Yahoo! News.
[6] Park, S. Park, and B. Oh. "User authentication protocol based on human memorable password and using rsa". In A. Lagana et al. (Eds.): ICCSA 2004, LNCS 3046, pages 698–707, 2004.
[7] A. Sasse, S. Brostoff, and D. Weirich. "Transforming the weakest link? A human/computer interaction approach to usable and effective security". British Telecom Technology Journal, 19(3):122–131, 2001.
[8] Prabhakar Gantela, Dr R.Mahammad Shafi,"Replacing passwords with Pass codes", International Journal of Computer Science & Communication Networks (IJCSCN), Vol 6(2), 94-97, ISSN: 2249-5789.
[9] Prabhakar Gantela, Tefera Adugnaw Luliee, "Self Authentication-an approach for password free authentication"- International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2763 Issue 10, Volume 3, October 2016.
[10] Prabhakar Gantela, Md.Mohammad Shareef. "Social engineering attacks and the counter measures"- International Journal of Innovative Engineering and Emerging Technology (IJIEET)- Volume 2, Issue 5, November-December 2016, Page No. 01-05 ISSN: 2455-3182