Personal Information Leakage During Password Recovery of Internet Services

The paper starts with the introduction of the people's life is entangled with the internet and how they cannot be separated. Every single person in the world has now brought their personal life to the internet and they use it as the medium of storage. For this purpose the certain internet service provide the facility of authentication, authorization mechanisms to make the users feel safe that their data is protected well. But when the users forget their password, passcode or any other authorization process they have to go through a recovery mechanism so they can gain access for their account. There are certain methods which are followed by most of the internet services which proves to be not so safe and it even helps the attackers by providing personal data.

Let us see what all are the information an attacker can collect with help of the data leakage. Alternate email, friends identities, age, education, phone number, location, personal identity these are the valuable information an attacker can get while the password recovery mechanism. Based on the domain name of the email such as .edu or .com the attacker can know whether the person is from an educational institute or not. When the recovery is through friends group then the attacker can guess locality, age, what kind of society he has joined based on the group of friends he has. If the recovery is through the phone number then he knows the last three digits of the phone number. Once he gets to know the locality of the person he might even know the first three number (usually the area code) of the phone number too. So the remaining 5 or 4 digits can be easily guessed with the brute force method or any fruitful methodology.

The third part of the paper discusses about the each services and what method of recovery mechanism each of these services provide. Facebook provides two ways of recovery mechanism. First is through the preexisting account such as email, Google account, and phone number. This might reveal certain information such as user's full name, educational institute etc. If it is through phone number then it can reveal last 2 or 3 digits for the user identification. Second method is through friends. Where three friends from three group are chosen and the authentication message is sent to them. If the attacker is close to the user he/she can contact those friends and he might even act ethically and can get the authentication message from those friends.

Gmail and yahoo provides the recovery method of either through phone or through alternate email address. During these process the Gmail shows the last 2 digits of the phone number, it shows the first and last letter of the email and the domain name for the alternate email address. These are considered to be the personal information too. PayPal uses the verification link process where the send the link to the user's registered mail and then by clicking on the link they are redirected to PayPal again to set the new password.

Attacks for these kind of method can be done by simply installing a third party application in the users mobile. When the application is installed it might ask for the permission to read the SMS and email from the mobile which might not seem suspicious to the user. Once the permission is granted the attacker can easily read through the SMS or the email of the user when he wants to gain personal information through any internet services. By this way the attacker can easily reset password and gain access.

Vignesh Kumar Karthikeyan Rajalakshmi

(A20424508)